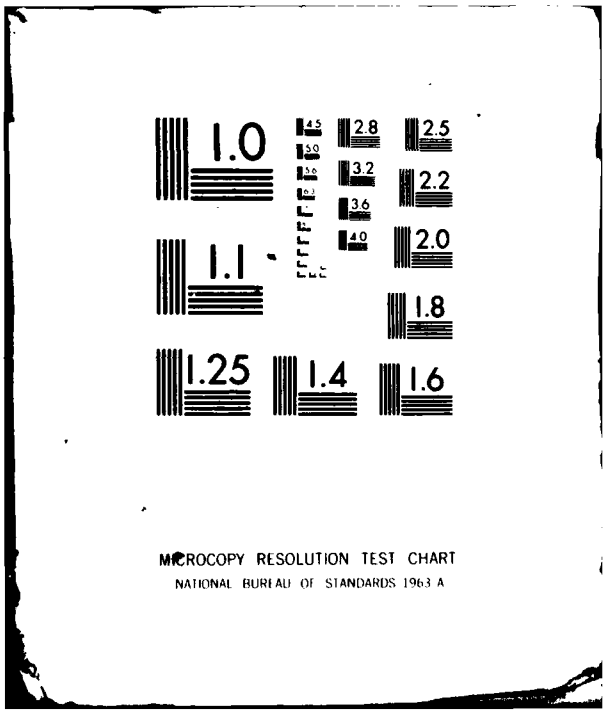
AD-A089 204 RANN INC PALO ALTO CA F/G 13/12
EXPLORATORY STUDY OF HAZARD MITIGATION AND RESEARCH IN THE AIR --ETC(U)
MAR 80 R L BISPLINGHOFF, P G DEMBLING EMW-00432
UNCLASSIFIED NL


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

FEDERAL EMERGENCY MANAGEMENT AGENCY

OFFICE OF HAZARD MITIGATION AND RESEARCH

EXPLORATORY STUDY OF HAZARD MITIGATION AND RESEARCH IN THE AIR TRANSPORT SYSTEM

March 31, 1980

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A089 304
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) Exploratory Study of Hazard Mitigation and Research in the Air Transport System.	5. TYPE OF REPORT & PERIOD COVERED Final Report.
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) R. L. Bisplinghoff, P. G. Dembling, A. J. Eggers, Jr., C. W. Harper, J. D. Young	8. CONTRACT OR GRANT NUMBER(s) EMW-0-0432
9. PERFORMING ORGANIZATION NAME AND ADDRESS RANN, Inc. Court House Plaza Building 260 Sheridan Ave., Suite 414 Palo Alto, CA 94306	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit 2361A
11. CONTROLLING OFFICE NAME AND ADDRESS Federal Emergency Management Agency Washington, D.C. 20472	12. REPORT DATE March 31, 1980
	13. NUMBER OF PAGES 87
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) Federal Emergency Management Agency Washington, DC 20472	15. SECURITY CLASS. (of this report) Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Technological hazards, disaster, air transportation, air transportation system, aviation, accident avoidance, aircraft accident li

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

New. HII 929

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Key Words

Technological hazards, disaster, air transportation, air transport system, aviation, accident avoidance, aircraft accident liability, insurance, negligence, design, construction, inspection, maintenance, operation, communication modes, accident investigation, hazard mitigation, nuclear power.

Abstract

The study examines a series of principles that may effectively mitigate technological hazards within the Air Transport System. These principles are:

1. Precise design criteria and verification of the standards which relate to an airplane's operating environment;

2. Quality control in manufacturing with high levels of performance in design, construction, inspection, and maintenance of the system;

3. Periodic testing and evaluation of equipment and human elements to meet performance standards;

4. Training and education of key managers and operators in emergency procedures with emphasis in new systems and multi-problem hazards;

5. Establish communication modes linking key elements with institutions in the system to mitigate, respond, and recover from emergencies;

6. A system of reporting incident and accident investigations in a prompt manner to allow for a coordinated recovery; and

7. The system must be regulated, audited, and demonstrated frequently to protect public interest, including proper liability.

These principles are then analyzed in three areas in which successful hazard mitigation will reduce the effects of increased technological application. These topic areas include:

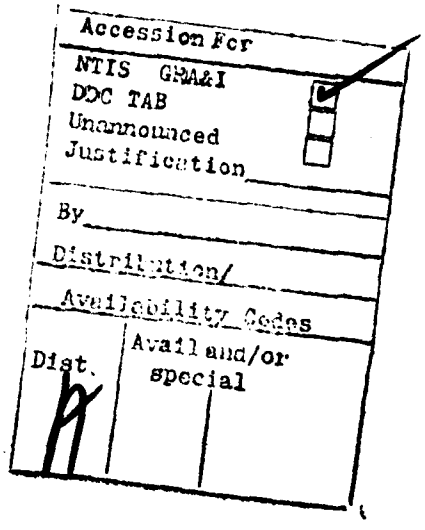
1. Design, Construction, Inspection, and Maintenance;

2. System Development and Operation; and

3. Liability and Regulation.

The study concludes that with the rapid development in high technology and with its subsequent rapid application to our → next page

National capability, technological hazards converge onto a wide variety of societies' activities. The report suggests that successful mitigation of technological hazards can be achieved through utilizing the previously outlined principles within the total air transport system environment.



EXPLORATORY STUDY OF HAZARD MITIGATION AND RESEARCH IN THE AIR TRANSPORT SYSTEM

By

R. L. Bisplinghoff
P. G. Dembling
A. J. Eggers, Jr.
C. W. Harper
J. D. Young

Submitted

to

Office of Hazard Mitigation and Research
Federal Emergency Management Agency

By

RANN, INC.

March 31, 1980

FEMA Contract Number EMW-0-0432

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The rapid developments in high technology and their equally rapid application to enhance our national capability and well being have led to a class of technological hazards which can portend disaster with no input from perturbed forces of nature. To be sure, of course, the technological hazards can be markedly exacerbated by natural phenomena, but they are fundamentally man made and ever threatening to unleash a disaster in the absence of their continuing careful control. These technological hazards now pervade a wide spectrum of societies' activities ranging from ground to air transportation, and from fossil to nuclear power generation and transmission. These hazards are an inevitable hallmark of an advanced technological society, and they can profoundly and adversely impact the material well being of the society if they either cease to exist (e.g., no air transportation or nuclear power generation) or if they go out of control (e.g., aircraft or nuclear power accidents). The answer, of course, is to develop and maintain effective management procedures for controlling these hazardous systems at acceptable levels of cost and risk.

It is to be expected that the emergency management of hazardous systems has problems in common. It is to be expected too that these problems may have solutions in common in terms of fundamental principles of mitigation and the problem focussed thrusts of research to deal with the hazards. It is important therefore to examine these principles and thrusts as they have evolved in advanced technological systems to date to clarify the lessons and principles

learned and their potential transferability from one system to another. Pursuant to this end an exploratory study has been made of hazard mitigation and research in the air transport system. The results of this study are the subject of this paper.

The air transport system was chosen for study because from the outset the development of aviation was dominated by the principles of "safety first" and "an ounce of prevention is worth a pound of cure." These were of necessity first principles because

a) Aircraft are inherently hazardous due to their extraordinarily high chemical,kinetic and potential energies of flight, and

b) Aircraft would be too heavy to fly at all if they were built with the overall structural weight and strength of surface transportation vehicles to withstand accidents.

Safety, therefore, has always been dominated by the goal of accident avoidance in aviation. As a result over the years there has been a steady decline of the idea that aviation is an ultra-hazardous and therefore highly limited activity subject to absolute liability or liability without fault for damage suffered in an accident. Thus too it was insurable at first only by a high risk-taker like Lloyds, London. Today the aviation activity is widespread, a major industry, and the air transport system is one of the safest and by far the largest commercial transport of passengers in the U. S. The activity is now covered by a broad base of insurance, and it is liable like other types of activity under the concepts of negligence. This has been accomplished only as a result

of the most careful continuing attention to hazard mitigation and research starting from design and carrying through construction to inspection, maintenance and operation of the system. It has evolved over some 50 years and today it involves a large, complex and sophisticated team of government, industry and university participants regulating, operating, constructing and researching the system and its elements.

This exploratory study of these various factors in the air transport system has served to highlight a number of principles that have been invoked and proven to effectively mitigate hazards in the system. Some key examples of these principles are as follows.

1. Precise design criteria and verification thereof must be employed which are carefully related to the total expected operational environment and the reliability of any new technologies employed in the system.

2. High levels of manufacturing quality control are absolutely essential, and uniformly high levels of performance are required in design, construction, inspection and maintenance of the system.

3. All key equipment and human elements in the system must be tested and certified as satisfying prescribed performance criteria for safe operation of the system. Manager-machine interactions are particularly crucial to precisely prescibe, test and certify near the safe operating boundaries of the system.

4. The training and maintenance of proficiency of key managers/operators in emergency procedures in the system is essential over the spectrum from incipient to ultimate emergencies. This cannot usually be satisfactorily achieved through use of the systems themselves and requires recourse to advanced simulation techniques, especially in dealing with new systems and multi-problem hazards.

5. Dedicated and precise communication modes must be provided and prescribed in the use to enable decisive and coordinated actions between key elements/institutions in the system to avoid, contain and recover from emergencies.

6. Timely and rigorous incident as well as accident investigation

and reporting is required to insure and maximize the benefits of experience in upgrading the effectiveness of hazard mitigation in the system.

7. The system must be continuingly regulated , audited, and demonstrated to be safe to the degree necessary to protect the public interest, including enabling adequate insurance of the manufacturers, owners and operators of the system liable for losses of people and property potentially exposed to accidents in the system.

It is suggested further by this study that one or more of these principles might well have important application to hazard mitigation in other advanced technological systems. These systems include movements of substantial amounts of hazardous material through a multi-modal transportation network, and generation and transmission of electric power through complex and extensive grids involving multiple power sources including fossil, nuclear, hydro, solar and others. Already there is evidence that the principles cited earlier on training in emergency procedures, dedicated and precise communication modes, and incident as well as accident investigation and reporting in the air transport system may have important application to hazard mitigation in the area of nuclear power generation. These and other potential applications deserve further study.

More generally it should be noted again that this study of hazard mitigation and research in the air transport system has been exploratory in nature. The experience gained with this system has been far richer in lessons learned than what is described herein, and it is still evolving. The air transport system is clearly one of our "gold mines" of knowledge on effective comprehensive emergency management systems, and it should be plumbed

for all of this knowledge and wisdom that it can provide in helping to mitigate the hazards of other advanced technological systems.

INTRODUCTION

Throughout history disasters have been associated with natural phenomena. Such events as hurricanes, floods, earthquakes and volcanic action have resulted from forces largely beyond man's control or cause. As urban and industrial development accelerated, a new class of disasters appeared stemming from human activities which compounded the effects of natural phenomena. Multistory buildings were built that were vulnerable to earthquakes, dams were built that sometimes proved unable to withstand flooding pressures; deep mines were developed which were sometimes poorly ventilated leading to dangerously foul air and occasionally to explosions causing their collapse; ever larger and faster ships were built which sometimes failed outright due to excessive structural loads in a severe storm, or outran their navigation capabilities and were destroyed through collisions in foul weather.

In more recent times the rapid developments in high technology and their equally rapid application to enhance national capability and well being have led to a new class of technological hazards which can portend disaster with no input from perturbed forces of nature. To be sure, of course, these technological hazards can be markedly exacerbated by natural phenomena, but they are fundamentally man made and ever threatening to unleash a disaster in the absence of their continuing careful control. These technological hazards now pervade a wide spectrum of society's activities ranging from ground to air transportation, and from

fossil to nuclear power generation. These hazards are an inevitable hallmark of an advanced technological society, and they can profoundly and adversely impact material well being of the society if they either cease to exist (e.g., no air transportation or nuclear power generation) or if they go out of control (e.g., aircraft or nuclear power accidents). The answer, of course, is to develop and maintain effective management procedures for controlling these hazardous systems at acceptable levels of cost and risk.

Such management procedures can only be evolved from Mitigation and Research (M & R) programs designed to develop and apply new scientific and engineering knowledge to predict, prevent and respond to emergencies and disasters so as to reduce the loss of life, injury, damage and economic and social disruption from such occurrences. It is not surprising, therefore, that many public and private groups associated with the development, application and control of hazardous new technologies have also developed programs in Mitigation and Research aimed at preventing or ameliorating the impact of disasters associated with these new technologies. Most recently, in recognition of the rapidly growing but widespread nature of the federal efforts in emergency management including M & R, the President acted with Congress to consolidate many of these activities with the formation of the Federal Emergency Management Agency (FEMA) in the summer of 1979. This Act enabled strengthened oversight and interchange of knowledge and experiences between many federal activities in M & R

which had been heretofore pursuing relatively independent paths. In addition it provided a federal focal point for interaction with state and local governments and private institutions concerned with similar emergency management problems.

It is to be expected and it is to some extent known that the emergency management of hazardous advanced technological systems has problems in common. It is to be expected too that these problems may have solutions in common in terms of the fundamental principles of mitigation and the problem focussed thrusts of research to deal with the hazards. It is important therefore to examine these principles and thrusts as they have evolved in advanced technological systems to date to clarify the lessons learned and their transferability from one system to another. Such an undertaking offers the general promise of upgrading multi-system safety in a foreshortened time frame, and the specific promise of systematizing and focussing M & R activities across the spectrum of current and evolving advanced technological systems. The undertaking is therefore of particular importance to FEMA in discharging its overall M & R responsibilities, and this paper attempts to contribute to this undertaking by examining selected aspects of the experience gained with major elements of the civil air transport system.

BACKGROUND

The age old principles of "Safety First" and "An ounce of prevention is worth a pound of cure" dominated the flight of aircraft from its successful inception. The logical supremacy of these principles was uncontestable at the outset since such a

machine could barely fly safely, and it could not fly at all with more than minimum structural weight and factors of safety (like 1 1/2 based on yield strength of materials), and with less than adequate propulsion thrust to weight ratio (like 1/10 based on maximum propeller and power plant performance) to meet critical flight needs like take off. In addition, the machine had to be controllable, if not stable, under perturbed or transient flight conditions if it was to successfully complete its journey, and therefore it had to be a predeterminably distortable load bearing structure. All of these factors had to be accounted for from the beginning by the Wright Brothers in successful flights of several hundred feet at Kitty Hawk almost 80 years ago, and through Lindbergh to today in successful flights of many thousands of miles over the earth's surface. Lindbergh pioneered further in the emergency management of aircraft because his flight across the Atlantic stressed the requirements to "not run out of runway in takeoff or landing," and "not run out of gas or altitude en route to the landing." To this day, with all the sophisticated advances which characterize modern aircraft operations, we cannot say that the air transport system is devoid of instances where such basic requirements are not met. This is not because the system is lax on the discipline to learn from experience - indeed it is among the most, if not the most demanding in this respect.[1*] Rather it is because the system is becoming ever more complex, and hence

*All superscript numbers refer to references which are listed at the end of each section.

ever more demanding on the hardware (the machine) to be managed, and the software (the humans) to manage it effectively. Both the single aircraft and the system of aircraft have always posed fundamental and never ending problems in emergency management, and this is why they are important to examine for their larger implications, their fundamental lessons if you will, in the field of hazard mitigation & research.

The airplane of today is fundamentally hazardous because its chemical energy (fuel), its kinetic energy (motion), and its potential energy (altitude) can be large by comparison to the binding energy of the parts of the machine and the people in it. Indeed it can be hazardous on any one of these counts taken alone, and taken together it can be deadly when out of control. It can be deadly to the people in the machine, to the people in other machines in its vicinity, and to people (and property) exposed to it on the ground. This multiple risk was not always of major concern. In the early days of flight there were so few aircraft in operation in relatively remote areas that they were primarily dangerous to themselves. Put more quantitatively, the mean free paths between multiple aircraft, and between single aircraft and people on the ground was so large as to minimize the multibody accident risk. The exception was at, or in the immediate vicinity of an airport, and there the people and property at significant risk were so involved only because they were dedicated to the operation. Thus, too, in the early days the most effective technologies evolved largely from the kite and the bike to yield cloth-covered stick and wire structures with chain drives from engine to propeller. Airfoils and propellers for aerodynamic lift and thrust,

respectively, were designed by "French curve;" navigation was by eye and compass, and flight control and hazard mitigation was by eye and "seat of the pants" feel. Flight weather was considered good only in the daytime when the air was clear and still, or at least steady in a low wind condition. Maximum flight speeds measured in the tens of miles per hour and flight altitudes in a few thousands of feet. Two people in an airplane were a lot, and research was still largely in the cut and try mode with flight articles. Indeed, the early innovations of Lilienthal and the Wright Brothers to use wind tunnels for aerodynamic research did not gain substantial momentum in the U. S. until the First World War with the advent of the National Advisory Committee for Aeronautics, and even then they did not appear in substantial number or size until well after the War. Airplanes did appear in large quantities during the war,* however, and the losses in human life and equipment due to accidents often exceeded those due to combat. It was inevitable therefore that accident investigation and reporting should emerge as a requirement to upgrade operational safety. This and much more carried over from military experience to civil aviation subsequent to the war, and indeed the history of aviation is replete with examples of constructive couplings including technology transfers between the military and civil sectors of air transport. These couplings are fundamental because both sectors are supported by many of the same research

*The first bombing raids involving hundreds of planes occurred over the Continent during the First World War.

institutions (e.g., NACA/NASA, Universities and Industries) and by many of the same manufacturing institutions (e.g., air frame, engines, et al). A particularly dramatic recent technology transfer has been the jet airplane from the military sector (KC-135) to the civil sector (Boeing 707), and this transfer has been built on over the last 20 years to the point where today U. S. manufactured jet aircraft dominate commercial aviation all over the free world, and commercial air transport dominates over all other forms of commercial passenger transport in the U. S.*

These transports can and do fly most any time of the day and night in most any kind of weather. They take off and land at airports in as little as 1 minute intervals, and there are hundreds of them in the air at any one time over the U. S. carrying tens of thousands of passengers at high subsonic air speeds. They fly from a few hundred to many thousands of miles and their departing and arrival airports are usually close to or in highly populated areas (cities or metropolitan areas). Thus commercial aircraft tend to congest in the air over congested ground areas so their mean free path is less while their potential (off course) closure rate is higher. Thus too the basic physical parameters have changed dramatically to increase multibody accident risk. The same can be said for the single body (aircraft alone) risk. Thus, for example, the jet transport of today has some two orders

*Indeed, the jet transport has been unique in moving the public perception of flight risks and benefits towards consonance with the realities of these factors. The jet transport dominates passenger service in terms of both passengers and passenger miles travelled per year.

of magnitude greater chemical energy and kinetic energy* than early aircraft, and an order of magnitude greater potential energy* in cruise flight. Yet, with all this, the commercial jet transport is one of the safest forms of transportation today. This is the case because it has never departed from its guiding principles of "Safety First" and "An ounce of prevention is worth a pound of cure."

Hazard Mitigation and Research on new technology have gone forward hand in hand with the development of the commercial air transport system. Technically, longer life materials with ever increasing strength-to-weight ratios and stiffness have been developed; lighter weight and longer lasting structures with fail safe modes wherever possible have been developed; aerodynamic designs have been revised and refined and power plant performance has been markedly increased** to greatly enlarge the flight envelope (speed vs. altitude). Flight controls now are powered, provided with redundancy, and frequently automated; navigation is aided by radio and inertial devices on board the aircraft, and it is under radar monitoring and direction from the ground at all times over the continental U. S. In the vicinity of airports (i.e., terminal locations) flight path control of individual aircraft resides with air traffic controllers on the ground in all but emergency cases. Primary and alternate communication channels are fully dedicated

*This is energy per unit mass. Including mass effects, the energy increased by another two orders of magnitude.

**The jet engine of today operates at many times the horsepower of the largest reciprocating engines for aircraft, and it is far more reliable (some five times higher MTBF).

to the continuing operation of the air transport system.

More generally the air transport system is designed with crucial redundancy to mitigate hazards. For example, all aircraft in the system are multi-engine and they can fly with at least one engine out. Moreover, they have sufficient fuel reserves to fly to alternate airports in case the primary airport is unuseable. These and other redundancies like those in navigation and flight controls noted earlier are effective in mitigating hazards and they extend to the human factor including a co-pilot. They are the product of years of experience with the "ounce of prevention" principle, and more recently they have evolved from the widespread application of anticipatory multipoint failure mode analysis.

With all this attention and sophistication in research and design to mitigate hazards in the air transport system, the firing line for putting "Safety First" still remains with the Federal Aviation Administration (FAA) in certifying flight crews, air traffic controllers and aircraft for operation in the system. The aircraft must meet established flying qualities requirements, the crews must meet corresponding flying capabilities requirements, and the controllers must meet the associated air traffic management requirements to be certified for operation in the system. Moreover, each is subjected to periodic recheck to verify that their performance is still up to the requirements. In addition the system is subjected to continuing oversight by the National Transportation Safety Board, including accident and incident investigations to maximize the visibility and corrective actions on lessons learned to avoid future hazards. Finally the Civil

Aeronautics Board (CAB) under the President determines the available routes and maximum allowable air fares for the carriers pursuant to engendering healthy competiton and to avoiding uneconomic and potentially unsafe operations. Thus the roles of regulation as well as liability figure nontrivially in the hazard mitigation equation.

In the event of actual equipment malfunction in flight, a number of safety measures have been incorporated on board the aircraft in the system. Thus emergency oxygen is available in case of cabin depressurization. Fire retardant and suppressant materials are available and employed to contain this hazard, and ignition sources (like lighted cigarettes) are restricted when the hazard is greatest during takeoff and landing. Seat belts are standard to restrict hazardous free body motions during takeoff and landing and other periods of potentially violent maneuvers, and emergency exits are provided from the cabin to permit rapid evacuation in case of landing accidents. In general at airports dedicated fire fighting and rescue service is provided in case of emergencies. In addition, passenger flotation gear is provided in case of emergency descent in overwater flights, and cabin crews are well trained in the emergency procedures to be followed with the passengers in the event of onset of any one of these hazards. As important as these procedures are, even more important are those that deal with the management and indeed the manageable state of the aircraft in its hazardous mode of operation. This brings us back to its original design and construction including maintenance, and its ultimate development and operation in the system.

As a general rule these functions are least demanding and least hazardous for the steady state portion of flight - i.e., the cruise phase.* By definition the rate of change in the dynamics of the aircraft system is at a minimum in normal operation in this phase, and hence the normal problems of management by the flight crew are at a minimum. Therefore, in the event of equipment malfunction crew distractions are at a minimum, the flight altitude is at a maximum, and so crew time available for corrective action is maximized. Much impending weather is directly visible with on-board radar while other weather, like clear air turbulence (CAT), is a continuing cause for concern. If the margins of safety are too limited at the cruise condition in the flight envelope, this concern can be of major hazardous portent.

Rate of change in the dynamics of an aircraft is dominant in terminal locations, i.e., in the vicinity of departing or arriving airports. On take-off the departing aircraft is under full power leaving the ground behind, so it is in a hazard reduction mode barring power plant or other basic functional failure. In landing the arriving aircraft is at reduced power approaching the ground, so it is in a hazard amplification mode. But both operations are at relatively high hazard levels because the aircraft must be managed under simultaneously changing conditions of speed, altitude, attitude and configuration (e.g., wheels and flaps location) in a relatively high risk environment characterized

*Aircraft design and performance in the cruise phase is most often determining of the efficiency rather than the safety of transport aircraft.

by relatively low mean free paths between adjacent objects like other aircraft and the ground. Thus, even under normal operation the flight crews and air traffic controllers are at their busiest managing change in landing and takeoff operation, and it is therefore no surprise that the system is stressed to a maximum with the add on of abnormal events under these circumstances. It is no surprise either, therefore, that aircraft accidents and incidents are most prevalent in this environment, and the consequences are usually most far reaching to people in the aircraft and on the ground.[2]

The specific causes and effects of these hazardous events are highly varied wherever they occur. They are important to understand, however, because they crystalize underlying causes and effects and fundamental corrective actions which are most likely to have applications to the effective management of a spectrum of hazardous advanced technology systems.[3] This paper has, therefore, been organized as follows. First, some fundamental aspects of the design and construction including maintenance of the air transport system will be reviewed with particular attention to key events including technological advances which have figured prominently in its evolution. Second, the development and operation of the system will be examined with emphasis on specific accidents/incidents which bring out underlying causes and fundamental corrective actions to be taken. Then some key issues of liability and the role of regulation in the development of the system will be reviewed, and finally some perceptions will be developed regarding the potential applicability

of experience gained from the air transport system to M & R on other hazardous advanced technology systems.

REFERENCES

1. Aircraft Accident and Incident Notification, Investigation, and Reporting. Department of Transportation, Federal Aviation Administration. July 16, 1976.

2. Linsley, Clyde Jr., Sorting Out the Crowds in the Sky - FAA Searches for Ways to Prevent Collisions, Transportation USA, United States Department of Transportation, Winter 1979.

3. Green, Richard J., Statement by Associate Director for Mitigation and Research, Federal Emergency Management Agency, Hearing before the U. S. Senate Committee on Commerce, Science and Transportation, December 11, 1979.

DESIGN, CONSTRUCTION, INSPECTION & MAINTENANCE

Introduction

It has been pointed out in the Background Section of this report that the jet transport of today is unique in that it combines in one vehicle an extraordinarily high level of chemical, potential and kinetic energy. These high energies exist, of course, in order for the jet transport to perform at high levels in terms of speed, range and altitude. High levels of performance in aircraft exact other requirements, the principal one being a vehicle of minimum weight. Although "Safety First" has been pointed out as a guiding principle in the air transport system, the designer of the flight vehicle is faced with the anomalous problem of designing for the smallest possible factors and margins of safety which are consistent with acceptable risk to the passengers.[1] Because of the uniqueness of these requirements, the air transport vehicle presents a useful device to study to obtain a better understanding of the principles available for mitigation of hazards in engineering systems.

Design and Construction

Design Criteria - Since the first powered flight of the Wright Flyer in 1903, engineers have steadily increased their knowledge of the criteria required to design aircraft so as to optimize their performance and minimize the hazards attendant to their operation. A detailed accounting of aircraft design criteria is beyond this report, but it includes such matters as maximum maneuvering accelerations likely to be sustained by a vehicle in flight, maximum

wind gusts likely to be encountered, loads produced during landing and taxiing, the margins required between speeds of aeroelastic instability and the maximum speed of the aircraft, required factors of safety and others. Every new aircraft is designed from carefully conceived design criteria which, in the case of civil aircraft, are promulgated by the Federal Aviation Agency.

Evolution of Design Criteria - Design criteria for aircraft have evolved from 75 years of operational experience and research. In the early days of powered flight, new flight conditions were not infrequently encountered that exceeded the design capability of the machine. For example, one of the earliest attempts to fly by Samuel Pierpont Langley failed because the wing was unable to withstand the loads placed on it during take-off. Flight loads placed on aircraft by maneuvers and gusts were at first crudely observed in flight and were later meticulously measured by flight recorders during operational flying. Thus, much of today's design criteria was gathered from flight experience. However, extensive research has contributed also to the present fund of knowledge. This research has been conducted in flight and in laboratories by government, industry and the universities. It has involved a wide variety of facilities ranging from research aircraft to wind tunnels, simulators and special purpose facilities such as a landing loads facility. Leadership in the development of design criteria for aircraft has been provided by the federal government, notably, through the NASA (and its predecessor NACA), the FAA (and its predecessor CAA) and the military services. Motivation for this

leadership by the FAA and the military was their need to specify design criteria for requirements and specifications of new aircraft. The NACA and NASA provided leadership through their charter as the federal agency for the conduct of basic aeronautical research.

Influence of Design Criteria on Hazard Mitigation

No engineering system exhibits the importance of rational and precise design criteria more than the airplane. Atmospheric flight without such criteria would at best be extremely hazardous and pose unacceptable risks to the general public. The history of the development of the air transport system is filled to the brim with examples of incidents which involved aircraft encountering new conditions for which they were under-designed. One example, pertinent to civil aircraft will suffice to illustrate this point. During the first fifty years of aircraft design, aircraft structures were designed like bridges and buildings for loading conditions produced by single maximum loads. For example, the design of the wing for atmospheric gusts was based on encountering a single large gust with a magnitude of approximately 50 ft/sec. The gust magnitude was selected as the largest that was likely to be encountered during the lifetime of the airplane. No account was taken by the designer of the fact that the airplane encountered daily many gusts of magnitude less than 50 ft./sec. The effect of repeated small loads on the aircraft structure was neglected. This philosophy of design produced reasonably satisfactory results until after World War II when new commercial aircraft began flying more hours than

before under more stringent conditions. In addition, newer materials of construction were introduced of supposedly higher strength. The loss of a wing on a Northwest Airlines Martin 202 aircraft in the immediate post-war period pointed up sharply the shortcoming of structural design criteria based on a single maximum load. It brought home a fact that was well appreciated in machine design, namely, that materials degrade under repeated loads due to fatigue. It brought out also the fact that some of the newer materials, in this case 75 ST aluminum, with higher ultimate strengths were no better than the older materials in their resistance to fatigue and fracture.

This unfortunate accident and a series of other similar events led the military services and the FAA to alter their design criteria to require that aircraft structures be designed hence forth for all loads placed on the structure during its lifetime. It thus became necessary for mounting a program to measure and predict not only the maximum loads likely to be encountered but all loads of any significance. The NASA, for example, devoted a major part of the effort of its Langley Laboratory to studying aircraft loads. Through the leadership of the NASA, design criteria for atmospheric gusts is now formulated in a statistical sense where atmospheric gusts are considered within the framework of a stationary random process.[2] This approach, which was borrowed from the statistical theory of communications, provides convenient design criteria whereby the designer can take account of the lifetime gust history of the airplane.

The post-war period brought out that structural design for a single load had provided a panacea for avoidance of other hazards. A by-product of such a design of early aircraft was a structure that not only had sufficient strength but also sufficient stiffness to avoid aeroelastic instabilities. But as aircraft speeds increased in the 1950's, it became evident that additional design criteria would be required to ensure that the lifting surfaces would be free from flutter within their range of flight speeds. The necessity for developing these criteria led also to major programs at NACA and NASA and to new approaches by designers.

Design Tools - Once the requirements on a new design are specified through design criteria, it is necessary for the designer to possess the tools necessary to translate these requirements into an engineering system which meets the criteria. Design tools are thus a fundamentally important link in the chain of events which must take place in creating a new airplane. Design tools include analytical methods of determining aerodynamic pressure distribution, methods of stress and aeroelastic analysis, fatigue and crack growth analysis, and many other analytical tools. In addition there are required computers and laboratory equipment for design verification as well as wind tunnels.

Figure 1 illustrates succinctly the design/development process as it applies to aircraft and aircraft engines.[3]

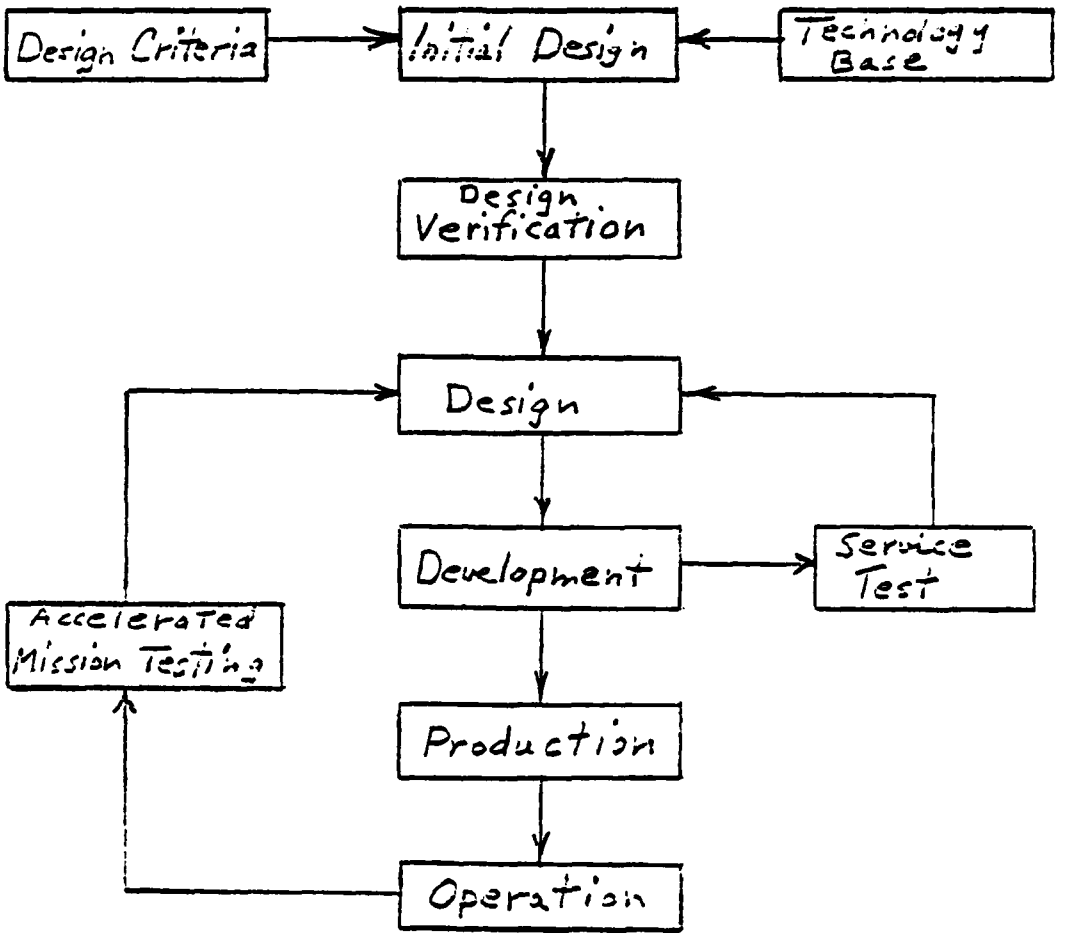


Fig. 1 - Design-Development Process

This figure is intended to bring out a feature of the tools of aircraft and engine design which has become a cornerstone of aeronautical and space development. This is the so-called "Design Verification System." The philosophy of design verification requires that each assumption used in designing a piece of hardware be verified by test and analysis to be certain that it is correct

before proceeding with full-scale hardware procurement and development testing. Occasionally an inexperienced program manager will skip this step to save money and he invariably finds that he is in trouble when the program reaches the system-integration stage. He frequently ends up in going back and carrying out the design verification process at a loss of time and increase in program cost. The technology base noted in Figure 1 provides improved materials, components, control systems, electronic systems, instrumentation and analytical tools. The aeronautical engineer who employs new technologies beyond those which have been demonstrated must identify and weigh the risks.

Evolution of Design Tools - Like design criteria, design tools have continuously evolved since the first powered flight. However, many tools used by aircraft designers are borrowed from other fields of science and engineering. For example, Miner's rule used in the fatigue analysis of aircraft structures as well as the powerful methods of fracture mechanics were both borrowed from mechanical engineers and metallurgists. On the other hand, the complex mathematical methods used to predict the speeds at which wing surfaces will flutter evolved from original work carried out by the NACA under Theodore Theadorsen at its Langley Field facility. In the past decade, the digital computer has had a profound influence on aircraft design. In the final analysis, its most important influence has been to allow the designer to reduce weight by designing closer to the requred design criteria with smaller margins and with less system redundancy. The purpose, of course, in doing

this is to maximize the performance and economic return of the aircraft. As we will see later in this section, this turn of events places an added burden on the construction, operation and maintenance functions since there is less margin for error in their performance.

Influence of Design Tools on Hazard Mitigation

As design tools evolved, numerous events occurred which illustrated that an engineering system like an airplane, which is designed close to its design criteria, must perforce be designed by very precise design tools. This point is illustrated by an example borrowed from modern gas turbine development. Like the airplane, the gas turbine has advanced spectacularly in the past 35 years. Many gas turbines have been designed to propel aircraft and ships, generate electrical power and provide energy for pipeline pumping. Turbine inlet temperatures have increased over 1000°F. Transport engine specific fuel consumptions have decreased 30% and propulsion system thrust-to-weight ratios have increased 250%.

While making major advances in basic engine technologies, there have necessarily been significant improvements in design tools. These are as important as the technology gains because the improvements in the effectiveness of the engine design and development process result in a more reliable and lower cost product. In the structural analysis of engines, recent advances include finite element methods, improved life prediction systems, design sensitivity analyses, engine vibration response analyses and integrated thermal design system analyses. In the measurement of

engine data during development testing, improved instrumentation in recent years provides sputtered sensor technology for strain and temperature measurements, laser radar technology for clearance and vibration measurements and full-scale-real time X-ray.

Using the tools available, the designer must make the best design he can using past experience and computer simulations, verified by design verification testing, and design the parts to operate reliably under the design criteria conditions. If the design tools are in error, the design will be unsatisfactory because the part will not be designed for the true speed, pressure, temperature or stress level at which it will operate. For example, in a modern aircraft gas turbine, an error in the predicted temperature gradient from the bore to the rim of a typical compressor disk could significantly change the life of the disk.[3] This is illustrated by Figure 2 which shows the relationship between bore to rim temperature gradient and low cycle fatigue (LCF) design life. In this case, a 100° F. error in predicted gradient would change the LCF life of the part by up to 50%. It is obvious from this example, that design tool precision is an absolute necessity in modern gas turbine design.

The philosophy of design verification employed by aeronautical engineers has served to highlight the problems of achieving designs that are fail-safe, fault tolerant, redundant or combinations of these until the design verification is well established on new technologies.

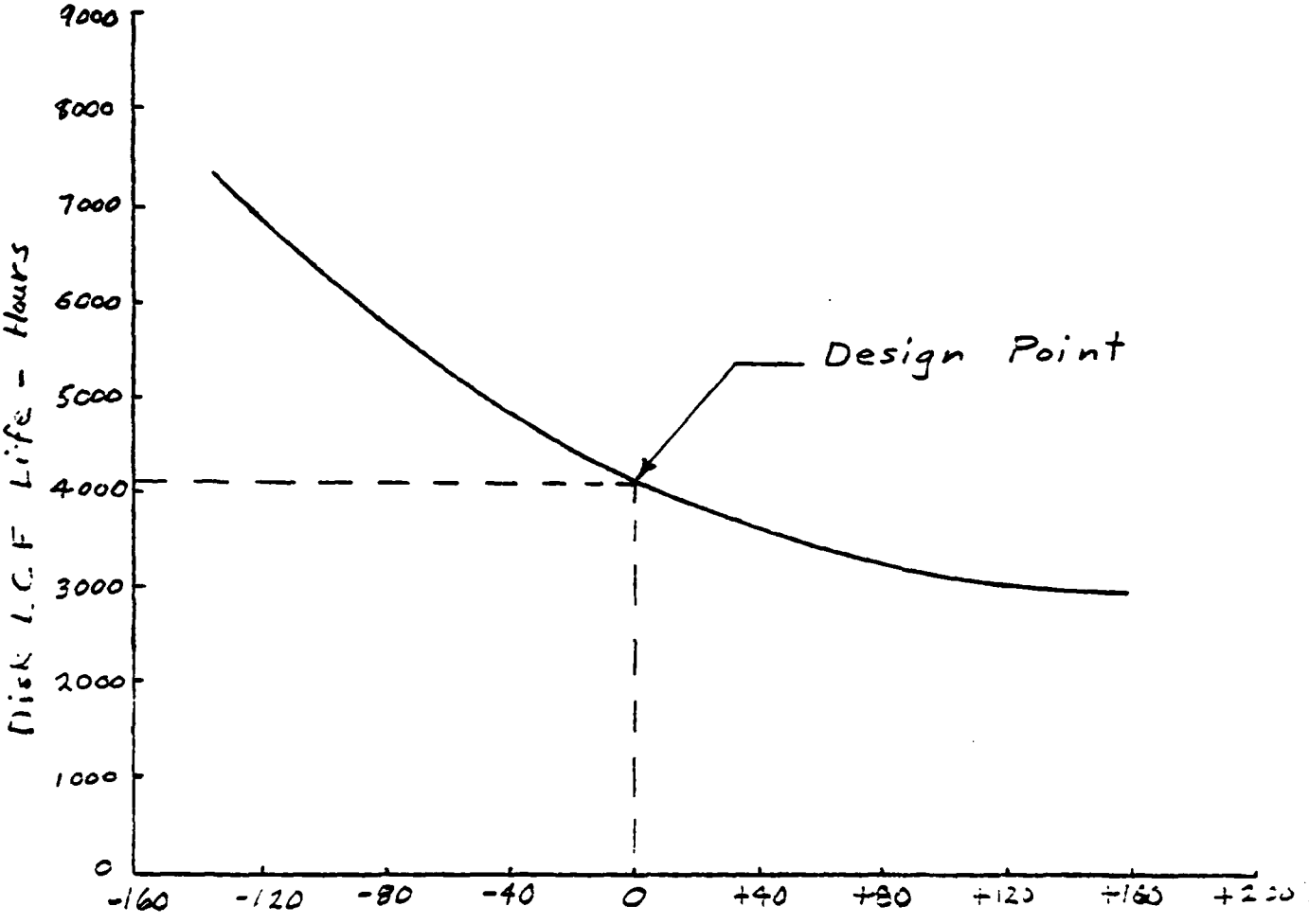


Figure 2. Change in Bore to Rim Temperature Gradient, °F

Construction

Even the most casual observer of aircraft over the years would note changes in the methods and materials of construction. Beginning with the materials of wood and fabric, moving to steel tubing plus wood and fabric, and then to aluminum, steel and

titanium monocoque construction, the airplane has continuously improved. At the same time, new tools of construction have evolved permitting the mass production of reliable and precise airframe and engine components and systems of minimum weight.

Of all the construction developments in the past two decades, the evolution of better strength and stiffness-to-weight ratio alloys and the numerically controlled milling machine have had the largest influence.[1] The phenomenal reductions in weight in airframes and engines are due in large part to the modern ability to remove all excess metal from a given component over and above that required to meet the design criteria. In a plant producing a modern high performance airplane, some 75% of the weight of purchased alloys leave the plant in the form of chips and 25% in the form of aircraft parts.

The modern ability to manufacture parts with precision and at low cost has had a profound influence on aircraft performance and cost. But these processes must be rigorously monitored and controlled by an exceptionally high level of quality control if the aircraft is to achieve its design objectives and at the same time be safe. Rigorous manufacturing quality controls are an absolutely essential element in the mitigation of the hazards of air transportation. This assertion has been demonstrated repeatedly over the years. The crack resulting in the wing failure of the Northwest Airlines Martin 202 mentioned earlier originated at a tool mark in a key wing fitting. Fasteners left out of important

fittings during assembly have been the cause of numerous aircraft accidents.

New methods of non-destructive evaluation have significantly improved quality control in the manufacture of aircraft and engines.[4] Nondestructive evaluation is the process of determining, without damaging them, whether the materials in products ranging from microelectronics circuits to nuclear reactors contain defects that would prevent their use. Present day nondestructive techniques, which are more art than science, are usually limited to giving qualitative information only - that is, they can indicate the presence of defects but cannot characterize them in detail. Although it is unlikely that this situation will change any time in the next few years, progress is being made toward more quantitative measurements. Better nondestructive testing techniques will improve our ability to design structures that perform close to the limits of the materials from which they are made. Vehicles designed in this way would be lighter and there would, of course, be savings in raw materials.

Inspection and Maintenance

When an aircraft becomes operational, the lead responsibility for hazard mitigation is handed off to the operator. In addition to measures to ensure safety during operation, there is also required a rigorous program of inspection and maintenance.

Commercial aircraft inspection procedures are specified by the Federal Aviation Agency for each aircraft type. Typically, the

normal inspection program has consisted of A (25 to 200 hours) and B (200 to 600 hours) checks consisting of close walk around inspections with emphasis on systems; C (1000 to 6000 hours) checks consisting of close walk around plus a close inspection of certain critical external and easy access areas with emphasis on systems and movable parts; D (6000 to 30,000 hours) checks consisting of a close external inspection of the entire airplane structure with detailed sampling inspection of 10 to 25 per cent of the internal-structure. In the past, initial and repetitive inspections were established on the basis of times found to be satisfactory or on earlier designs with some extrapolation that takes account of design improvements and a rating of criticality. The initial inspection program was then tightened in areas where service problems occurred and intervals extended where no problems were found. This procedure has generally been satisfactory except that it has not given adequate coverage for cracks growth rates in critical areas, or the increase of frequency and locations of fatigue cracking on aging structures.

But, the penalty for breakdown is severe. Hazard mitigation in aircraft is critically dependent on high quality inspection and maintenance performance. This point was illustrated tragically in June, 1979 when a DC-10 crashed at O'Hare Airport killing all of its 274 passengers and crew members.[5] A careful study of the cause of the O'Hare crash revealed that it resulted from structural failure of an engine pylon that was triggered by a 10 1/2 inch crack induced in the pylon rear bulkhead by a maintenance procedure

employed by American Airlines at its Tulsa base. The aircraft flew over 500 hours during which time the crack was not discovered and grew to 13 1/2 inches as a result of fatigue. Finally, the loads produced during the O'Hare take-off were sufficient to cause the crack to grow explosively resulting in the fatal crash. The O'Hare crash illustrated again that the modern jet airplane is unforgiving of casualness in inspection and maintenance

It should be evident from the previous discussion that hazard mitigation in aircraft requires a uniformly high level of performance in all of the important functions. Modern engineering is capable of producing after millions of man hours of effort a very efficient aircraft of high performance. But at the same time it is complex. The same high level of technical effort and attention to detail as was used in its design must be applied during construction, inspection and maintenance. This lesson is repeatedly learned from failure of sophisticated engineering systems by modern society, the most recent examples being the DC-10 accident at O'Hare and incidents with the Three Mile and Crystal River nuclear reactors. It is a fact that modern and sophisticated new technologies and design procedures are useless and unemployable if it is not possible at the same time to maintain and inspect these systems in such a way as to assure at all times the integrity and airworthiness of the system and its component subsystems. In assuring this integrity in commercial aircraft it is, of course, necessary to take into account the exigencies of inspection and maintenance under field conditions.

Conclusions

The following list outlines some of the main principles which are suggested by the overall experience gained in the design, construction, inspection and maintenance of the air transport system.

1. Complex engineering systems require precise design criteria carefully related to the expected operational environment.
2. Design criteria should reflect, whenever possible, the total anticipated operational experience in a statistical sense, not just the expected peak values.
3. Modern design tools permit designers to design complex engineering systems closer to precise design criteria thus making critical the importance of well conceived design criteria.
4. A philosophy of design verification is necessary. When new technologies are employed beyond those which have been demonstrated, designers must identify and weigh the risks.
5. High levels of manufacturing quality control are absolutely essential for safety and reliability.
6. For hazard mitigation a uniformly high level of performance is required in design, construction, inspection and maintenance.

REFERENCES

1. Boyne, Walter J. and Lopez, Donald S., The Jet Age, Smithsonian Air and Space Museum. Oct. 26, 1979.
2. Bisplinghoff, R. L., Ashley, H. and Halfman, R. C., Aeroelasticity, Addison Wesley Publishing Co., Inc., Cambridge, Mass., 1955.

3. McDonnell, B. J., The Application of a Design Verification System and Accelerated Mission Testing To Gas Turbine Engine Development, Society of Automotive Engineers Paper 780991, 1978.

4. Robinson, Arthur L., Making Nondestructive Evaluation a Science, Vol. 205, 3 August 1979.

5. Carlen, Wm. M., FAA Inquiry Charges DC-10 Manufacturing, Maintenance Mistakes, The Wall Street Journal, July 17, 1979.

SYSTEM DEVELOPMENT AND OPERATION

Introduction

Development and Operation of the air transport system has brought to the fore at least two problems which cannot always be examined fully in the design and construction of the elements of the system. First, the development and operation of the system and its elements is carried out by people who must be familiar with and actively involved with every element of the system as compared to the specialists who design and construct the many pieces of the total system. In short, this phase is the responsibility of the systems managers, and they must be specially trained to handle the system. Second, operation of the system brings many interactions between the various elements of the system into play, including especially manager-machine relationships, which cannot be truly quantified before the fact, because all the facts cannot be anticipated. For many years the mitigation and research associated with preventing disasters in operation were reactive, initiated and carried out only after a disaster had demonstrated the need. This has been effective in that it has been possible to identify the cause, to accomplish the research required for mitigation and implement it after the problem was evidenced by one or several very closely allied disasters. More recently, efforts have developed toward identifying potentially disastrous situations and providing mitigation before the event.

To illustrate the foregoing, 7 specific cases have been chosen for closer examination. If examined in great detail these events are different in nature and closely associated with the technology of air transport. However, in each of these cases can be found basic principles in hazard mitigation; these cases reveal the effects of introducing new design features (cases 1, 2, 3), of inadequate presentation of necessary information to operators (cases 4, 2), of ignoring limits in human sensory capabilities (cases 5, 3), of providing inadequate training in hazardous operations (cases 6, 4, 3); finally, a developing technique for moving from reactive to anticipatory mitigation and research is examined. (Case 7).

Case Studies

Case 1 - Information to Maintain Margins-of-Safety

On July 12, 1963, a four-engined jet transport climbed towards 40,000 feet in an effort to escape turbulence that was creating an uncomfortable ride. Instead of clearing the turbulence, it became more severe, the jet was exposed to large attitude changes and eventually entered into an uncontrollable dive from which it recovered only after nearly 30,000 feet of altitude had been lost.[1] This was not the first incident of this nature and was followed by several more, some of which led to fatal crashes. As a consequence the government initiated a series of investigations to study the nature of the turbulence appearing in clear air, the control characteristics of the various aircraft involved and the development of instrumentation which could provide the pilot with some warning

of an impending encounter with such turbulence. Some relatively minor changes in some of the aircraft types together with modified operating procedures eliminated such incidents. Nevertheless, much of the research and analysis continued and has produced findings of value to management of systems other than the air transport system. It is these that are of concern here.

To assess this value it is necessary to examine some underlying causes of the accidents in question. First, it needs to be recognized that a jet transport, like most technically advanced systems, operates most efficiently when each element of the system is operating near its limit performance; that is, failure will occur if more performance is demanded but underutilization exists if less performance is used. Yet a margin of safety must be maintained in the operation so that transients in the system do not drive the system into a failure situation. The operable limits of a jet transport in terms of cruise speed vs altitude have the form indicated on figure 1. To the left of the operable boundary the aircraft becomes uncontrollable because of stall resulting from air too thin to maintain lift at that speed; to the right of the boundary the aircraft becomes uncontrollable because of lift loss due to compressibility effects. The most efficient operation is at high altitude just between these boundaries. The maximum efficiency that can be aimed for is conditioned by the ability to approach but not exceed these boundaries. In the design of the aircraft, the maximum operating efficiency sought is that associated

with maintaining an adequate margin of safety, not an uncompromised peak efficiency. It is the responsibility of the federal government to satisfy itself through demonstration that the adequate margin of safety exists; this latter is constantly being adjusted as new knowledge and new experience, such as the case in question, is gained.

Beyond designing for maximum efficiency of operation with adequate margins of safety there is also the problem of informing the operator of precise operating conditions, particularly during transients, so that any corrective action taken serves to counter the transient effects and not reinforce them. This was eventually found not to be the case for the incident in question. Thus understanding, when reached, proved very revealing in connection with operator control of the system.

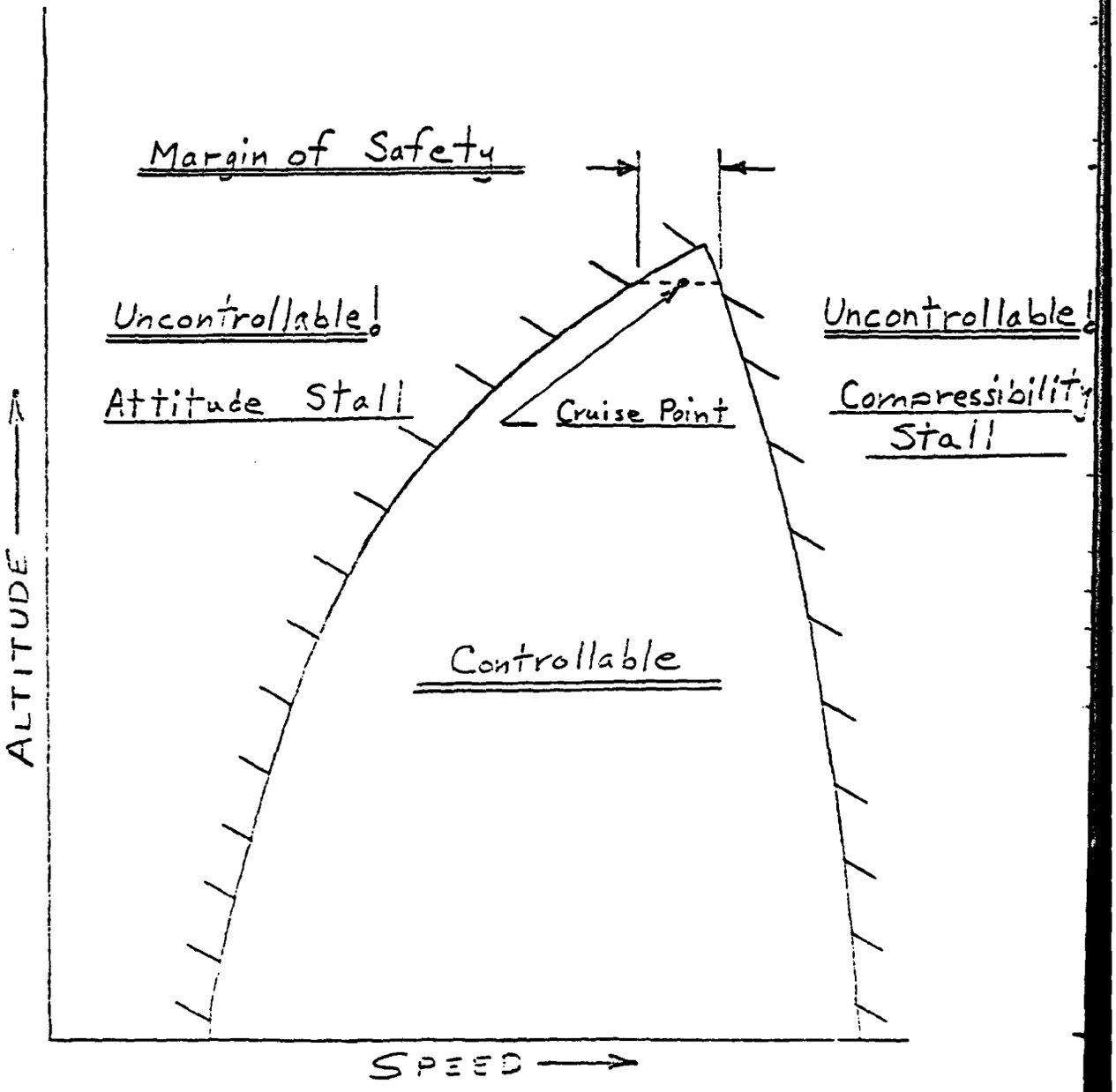
Of primary concern in safety of flight is maintaining flight speed between the minimum and maximum allowable. Direct measure of flight speed by the operator is not possible hence it must be sensed by other means and presented to him; since constant attention to flight speed is not practical, the operator takes advantage of the fact that attitude (nose up or down) is an indirect measure of flight speed which can be sensed both through the balance canals and through vision, even peripheral vision. This is true to a usable degree, however, only when any motion of the free air is essentially normal to the gravitational field. In turbulence, where strong vertical air currents exist, attitude is not a safe indication of air speed, nose up can occur with increasing speed

and vice-versa. It was found that, possibly because the direct air speed indicator was difficult to read during turbulence, the pilots were reverting to basic training procedures of controlling speed with attitude and actually aiding the turbulence in exceeding the margins of safety into the uncontrollable operating regime. Although much effort was devoted to study of more effective flight speed indicators, it was finally found sufficient to develop training procedures which allowed the pilot to use different flight control techniques when such turbulence was encountered. It is recognized that the use of differing control techniques for different conditions in itself introduces the possibility of confusion leading to difficulties. In general, the acceptable solution has been to increase the margin of safety by operating farther from the boundaries.

There are at least two findings of fundamental importance to the control of sophisticated systems which can be drawn from this experience.

(1) Extreme care must be taken to establish the system characteristics that establish the boundaries where a system may go unstable or uncontrollable and to determine the margin of safety which must be maintained in order that transients don't result in exceeding these boundaries. In addition some forms of system simulation and training are required to establish precise operating procedures to assure recovery if unexpectedly large transients bring the operation close to the boundaries.

(2) Information required must be clearly and unambiguously presented and should be used during all normal operations so



FLIGHT ENVELOPE

FIGURE 1

familiarity is maintained. Extreme care must be taken that basic human sensing capabilities, which may be misleading under emergencies, do not become a normal source of information during routine operation (sound, vibration, etc.). Clarity of information required in emergency conditions must not become confused in presentation during emergencies, even though perfectly acceptable during routine operation (properly positioned so not obscured or out of vision during actions to counter emergencies, etc.).

Case 2: Information Overload Through Hazard Warning

On 1 December 1974 a three engine jet transport crashed into a low hill 25 miles northwest of Dulles International Airport killing all 91 occupants and totally destroying the aircraft.[2] The aircraft was on a scheduled flight from Columbus, Ohio to National Airport, D. C. but while en route was diverted to Dulles Airport because of severe weather conditions in the National Airport area. On the approach to Dulles Airport the aircraft began its descent early, some 44 miles from the runway, dropped below the minimum safe altitude in the process and impacted a low hill at an altitude of about 1700 feet.

The investigation showed that there was no technical malfunction either in the aircraft, or in the air traffic control system, which played any part in leading to the disaster. While the weather was poor enough to severely impair visual contact with the ground, the investigation concluded that the weather played no important part in the accident. The conclusion finally reached through the investigation was that ambiguities in the communication between

the aircraft operator and the ground control were directly responsible for the disaster. When the operator was given clearance into the Dulles runway he apparently understood this also implied clearance to begin his descent whereas the ground control understood the clearance was only to continue his flight toward the runway until the approved descent point was reached. This difference in interpretation was not discussed explicitly in any of the communications between the aircraft and ground control. While the aircraft carried an altitude alerting system which through a radio altimeter gave aural warning of low altitude just before impact, it was the sense of the investigation that, with the descent rate established, the operator did not have time to avoid the accident after the warning was given.

The major part of the investigation centered around the ambiguities in communication between various elements of the system. Many were found and recommendations were made for a complete review of communication patterns to eliminate ambiguities. This problem is, of course, fundamental to the problem of managing a sophisticated and constantly evolving system. Each new capability introduced provides the opportunity for long established and clear communication procedures to acquire a double meaning with the ambiguity this implies. There is no question that communication in the control of technically sophisticated systems has become and will remain a problem that requires constant attention.

For the subject analysis, however, another action resulting

from this disaster is of special importance. Outside of the formal investigation a great deal of attention centered around the operator's failure to respond to the altitude alerting system in time to avoid the problem. In a perhaps simplistic approach, great pressure developed for rapid development and installation of an "adequate" ground proximity warning device which would "prevent" the operator from descending below a safe altitude. In response the FAA directed that all air carrier aircraft be equipped with such a device within one year.

This directive initiated much research into various systems to meet the goal. These ranged from systems designed to overpower the operator and force the aircraft to climb when ground proximity was sensed to systems that provided "over-riding" cues to the visual, or aural, or tactile senses that could not be ignored. Not surprisingly it was found that very complicated systems introduced the possibility of creating other hazards and the most that could be done was increase the sensitivity and strength of cue of the existing system. When this was done it was found that increased sensitivity produced false warnings and the stronger cues interfered with other activities to the point the operators were disarming the systems. This result brought into clear focus the fundamental problem of concern here.

As the aircraft had grown in complexity, so had the number of alerting systems grown to alert the operator of a malfunction. With the ground proximity warning system experience it became clear that the operators were reaching the point of information saturation. It was recognized further that new systems were coming

into being that would also require malfunction alerts. For these reasons research was initiated in two directions, that of combining alerting devices to serve multi-purposes and that of prioritizing alerts so that only those of primary concern to the particular operating state of the moment were armed. This logical approach obviously introduces some new problems. A way must be found to prevent any ambiguity in interpretation of an alert that is multi-functional. Clearly the operator cannot assume the task of adjusting alert priorities each time the system state changes. All of the research required to resolve these questions has not been completed. However, techniques for removing ambiguities in multifunctional alerts are being explored successfully. Failure or fault analysis of complicated systems is being extended to the problem of prioritizing alerts. The fundamental principles deriving from this air transport related work should be basic to the solution of similar problems associated with the avoidance of disasters during the operation and management of all sophisticated systems.

Case 3 - Inadequate Information on New Design Features

On August 16, 1965, a three jet transport crashed into the waters of Lake Michigan while making an approach to O'Hare Airport in Chicago. All 30 persons on board were killed. The aircraft type was new, having first entered service in February 1964 and had operated without incident up to the time of the subject crash. No clear evidence as to the cause of the crash was uncovered although it appeared as though a very steep descent rate was

established, from cruise altitude, which was not checked prior to the crash. While the investigation was proceeding, a second transport of the same type crashed on approach to Greater Cincinnati Airport on November 8, 1965, killing 58 of 60, again having established a high rate of descent which was not checked before impact. While evidence was being gathered on this accident, a third aircraft of the same type crashed on approach to Salt Lake City, again the evidence indicating an unchecked high rate of descent to impact. The final incident of the series occurred with a similar type aircraft on approach to Tokyo Airport where 133 persons were killed.[1]

A series of major investigations were instigated by industry and various elements of the federal government to examine every conceivable theory as to why qualified operators with extensive experience could have come to operate the aircraft in a manner leading to disaster. The aircraft structural and aerodynamic designs were reexamined and pronounced satisfactory; the training and operating procedures were reviewed and found satisfactory; the information provided the operators as to the state of the system were found equal to or better than given in the past. It was found possible to find a combination of events and circumstances to point to the cause of any one accident but none that were applicable to all.

It was only after some two years of study that the very subtle underlying cause of the accidents became clear. Aircraft wings create lift by virtue of imparting downward momentum to the

air as the wing passes through it; the greater the angle of the wing to the air, the greater the downward momentum and the lift. At some maximum angle the air ceases to follow the angle of the wing, separates from the wing.

Associated with this is a rapid increase in drag of the aircraft and stall with lift loss occurs. Many years of aerodynamic design development had established principles which assured that the operator was provided warning of impending stall and that aircraft motion after the stall automatically returned the aircraft to a controllable state.

The introduction of the swept wing jet transport introduced some subtle changes in stalling characteristics which are of special concern to this analysis. Both loss of lift and increase in drag associated with stall progressed much more gradually than was the case with unswept wing designs. To avoid operating in a partially stalled condition, the operation was confined to flatter angles and higher speeds, particularly during approach to landing. While this was safe for clear approaches to long runways it prevented operation into smaller airports surrounded by high terrain. The demand for jet transport service into such airports led to extensive aerodynamic research to remove this limitation. Devices were developed which markedly delayed the appearance of stall, and the increase in drag associated with it, thus enabling steep descent at slower speeds, the desired objective.

Use of these devices, however, intensified a form of drag

which had been relatively unimportant in previous operations. This drag-due-to-lift, or "induced drag", was not apparent to the operator through the buffeting associated with separation drag he had long been familiar with (See Figure 2). Thus the aircraft could be flown under good control in steep descent with no warning that very great increases in power would be required to overcome the drag and check the descent. It was this subtlety which had been responsible for the series of disasters. An im-improvement indesign which offered great operational benefits was negated by the inability of training to overcome long established and ingrained operating habits. When the problem was identified, many operators simply restricted use of the available performance increase; others intensified training and made some use of the capability but not under circumstances where other stresses of operation might cause the operator to revert to old operating techniques.

A vitally important lesson in the management of sophisticated systems can be drawn from this experience. The introduction of a new characteristic into an established system which alters the cues used by the operator to manage the system safely can easily obscure the information required to avoid disaster. In the subject case the technical aspects of the situation were examined in detail by highly skilled technical personnel both before and after the tragedies and still this critical human factors aspect was given insufficient attention. It is clear that even the most beneficial system changes must be examined critically in the light of prior operator experience and tendencies to revert to intuitive actions under stress.

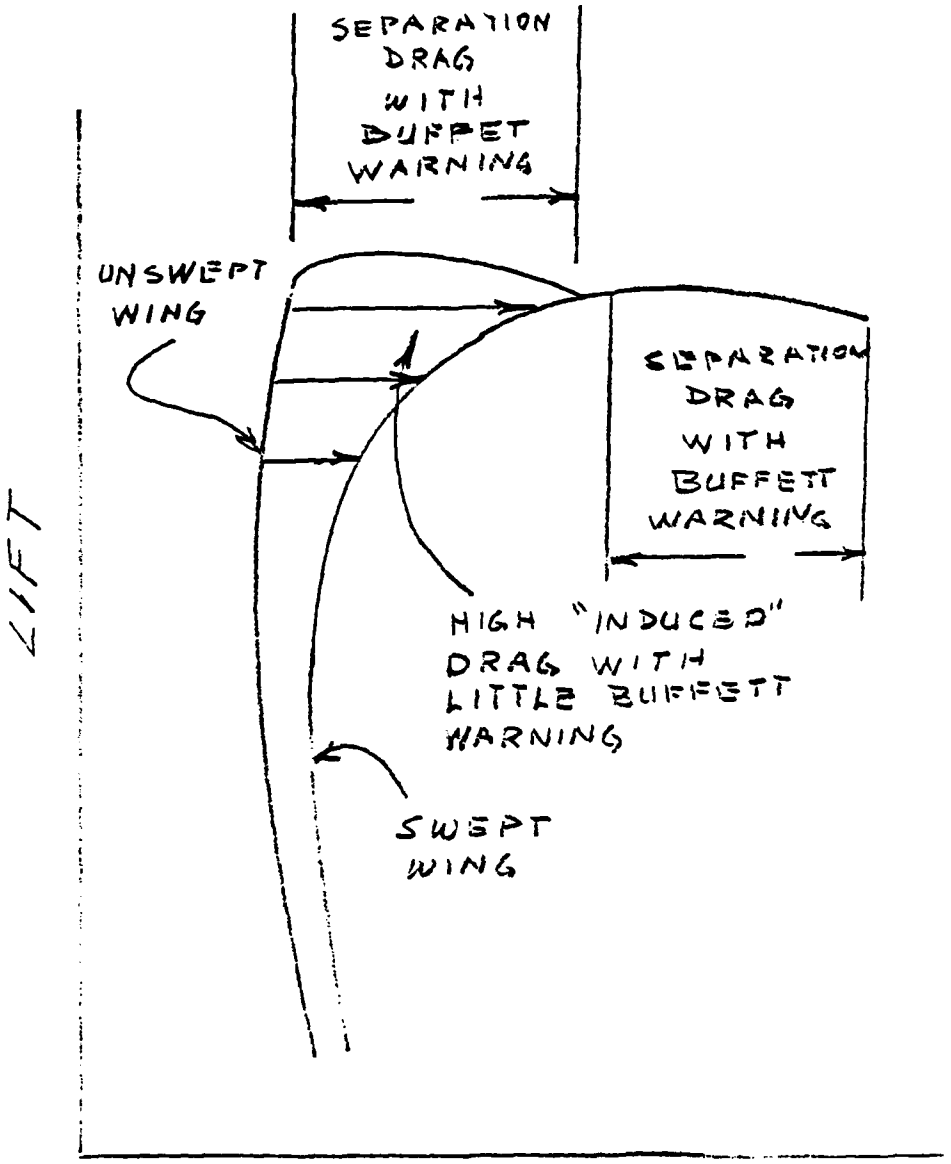

SEPARATION DRAG WITH BUFFET WARNING
UNSWEPT WING
SEPARATION DRAG WITH BUFFETT WARNING
HIGH "INDUCED" DRAG WITH LITTLE BUFFETT WARNING
SWEPT WING
LIFT
DRAG

FIG. 2

Case 4 - Improper Training in Resource Management

On December 28, 1978 a four engined jet transport crashed into a wooded area during a landing approach to Portland International Airport.[3] Ten persons were killed, 23 were injured seriously and the remainder of the 189 aboard escaped injury. The direct cause of the accident was fuel exhaustion about six miles short of the runway with all engines shutting down.

The aircraft was on a scheduled flight from New York via Denver to Portland. The flight was routine until preparing for the landing at Portland. When the landing gear was extended for landing the indicator lights failed to indicate proper deployment of the main gear. The pilot asked for and received clearance to "orbit" until the nature of the problem was diagnosed. For slightly over an hour the aircraft circled while the technical problem was studied, fuel was burned to reduce the chance of fire on landing and the crew prepared the passengers and aircraft for an emergency landing. When it was decided the malfunction could not be corrected, the pilot asked for and received permission to land. Although the approach path to the runway was established, fuel exhaustion occurred before the runway was reached and the crash resulted.

The investigation determined that the landing gear deploying mechanism had malfunctioned and that an emergency did, therefore, exist. The major interest in the investigation centered around the actions which led to remaining airborne until insufficient fuel remained to reach the airport runway. Two aspects of this problem were examined in detail, (1) the adequacy of the

information available to determine fuel available and (2) the use made of this information by the operators.

Precise measurement of fuel aboard is difficult to achieve in an aircraft. Yet accuracy is exceedingly important. Federal regulations require that sufficient fuel be carried to allow for delays at the destination or diversion to an alternate if the destination airport should be unusable. Economics of flight demand that excess fuel not be carried; increased gross weight requires increased thrust during flight with the result that fuel is wasted. Direct measurement of fuel on board at any time during the flight is not possible to the accuracy required to assure the existence of adequate reserves. Direct fuel measurements are, therefore, supplemented by a knowledge of fuel taken on board before departure and a constant recording of fuel flow rates during the flight to establish fuel remaining at the destination. Although considerable attention was given the problem of fuel - remaining determination in the investigation, that problem is not of major interest to the subject analysis.

The investigation showed that aircraft arrived at its destination with proper fuel reserves and that the operators were aware of this. Unworried about fuel, the crew turned their attention to two other high priority problems, ascertaining the nature of the technical problem and attempting to find corrective action, and making certain the passengers and cabin crew were properly prepared for an emergency landing if that should prove necessary. For all but the last few minutes of the hour the

aircraft was circling, the recorded conversations between the crew members themselves, and various ground based groups involved in seeking a solution to the technical problem, were centered around these two high priority problems. Except for initial assessment of fuel remaining at the start of the incident, scant attention was paid to this very critical matter until fuel exhaustion was evident from loss of power in one engine. Even at that point, some confusion was evident as to whether it was possible to transfer fuel between tanks to restore the lost power.

Review of crew training and experience disclosed nothing which would have foretold a potential problem of this nature. Nevertheless, primary cause for the accident was directed at crew actions. However, the accident did serve to accelerate and expand a number of small studies which had been analyzing group control of sophisticated systems. The general problem under study was categorized as cockpit resource management.[4] Perhaps the more pertinent elements of the studies insofar as this analysis is concerned are those directed at human factors. At least three questions under study are appropriate for far wider application than the aircraft problem. How is the ranking of authority established and accepted so it does not break down under stress? How is the division of responsibility specified so that, under stress, routine activities continue and are not overlooked to aggravate a problem? How is training conducted so that these established procedures are not disrupted by varying groups of operators which may contain personality clashes? Properly applied answers to these questions could well have prevented the

disaster under discussion. There seems little doubt that these same questions will arise in the control of other technically sophisticated systems. Solutions to these questions, and others of a related nature, are being sought through the development of simulations capable of reproducing real world stressful situations and directed by scientists skilled in understanding "human factors" problems. Close association with these research activities should be of great aid to those responsible for the mitigation of disasters stemming from actions of human controllers of modern systems.

Case 5 - Information Requirements in Excess of Human Sensing

On 24 June 1975 a jet transport touched down short of the runway threshold at Kennedy Airport; the impact occurred on a freeway adjoining the airport and 113 persons of the 124 on board were killed.[5] The impact occurred during a break in freeway traffic or the disaster would have been much greater. Weather conditions were severe, with rain and strong, shifting winds.

It was generally conceded that a strong shift in wind direction during the later stages of the landing approach created the problem: this condition had been reported by other aircraft operators just prior to the accident and one aircraft had aborted its landing for this reason. This type of incident was not new. In prior years shifting winds had been reported to have caused aircraft to miss their expected touch down point by a considerable distance (See Figure 3), some proceeding beyond and off the end of the runway, but without serious injury to passengers. The possibility of confronting this problem had long been recognized by regulatory bodies; for example, after the minimum landing distance had been

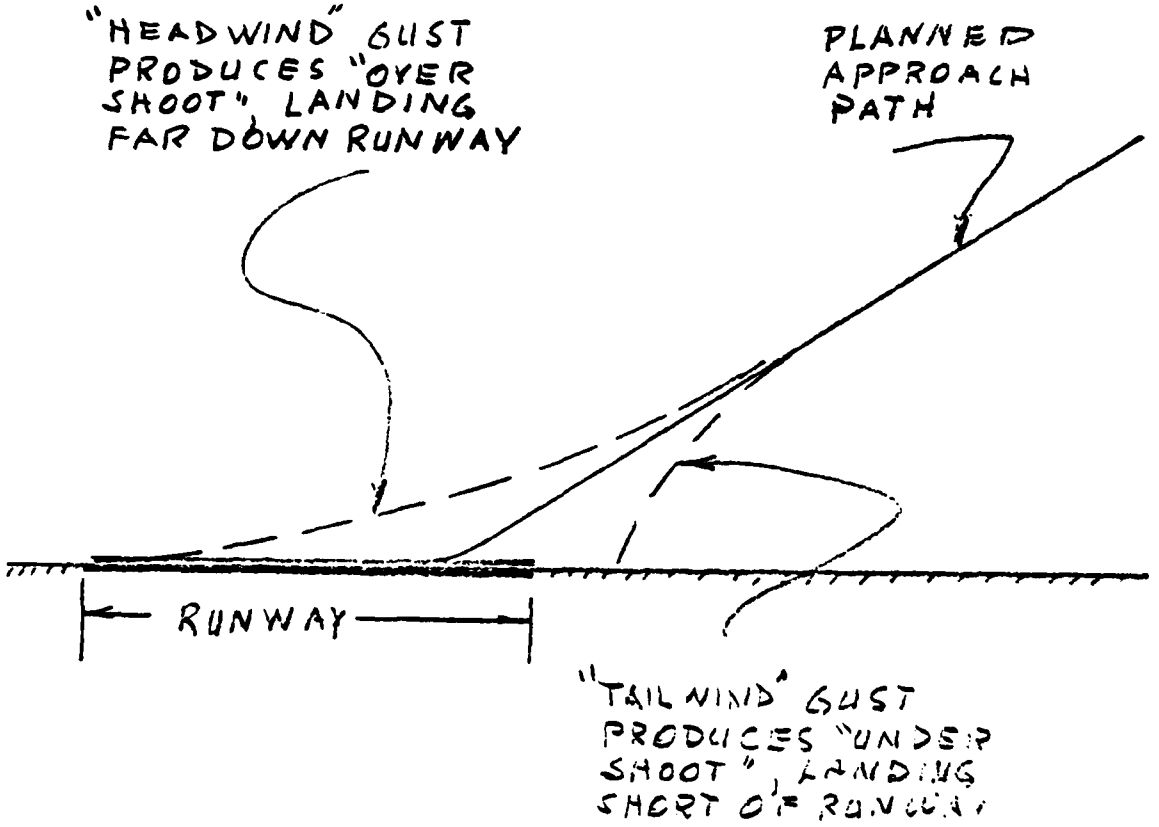

"HEADWIND" GUST PRODUCES "OVER SHOOT" LANDING FAR DOWN RUNWAY
PLANNED APPROACH PATH
RUNWAY
"TAIL WIND" GUST PRODUCES "UNDER SHOOT" LANDING SHORT OF RUNWAY

FIG. 3

established during type demonstration of a new aircraft, this distance was increased by an arbitrary percent to allow for wind shifts, among other factors, which might occur during operation.

The major focus of attention during the early stages of investigation of this incident centered around the operators competence as soon as it was ascertained that no system failures had been a contributing factor. Initially, the primary cause of the accident was attributed to operator judgment, particularly since accidents had been avoided in the past under similar circumstances. As the investigation proceeded, however, it became increasingly clear that operators were being asked to perform a maneuver for which they had inadequate information and that in those cases where the landing had been attempted and succeeded, luck had perhaps played a greater role than operator skill. Also, it was recognized that in the past an aborted landing was a more viable option to the operator than was the case in the present period of very crowded airport operations; use of terminal airspace and runways is scheduled far in advance and disruption of this schedule can create major problems in control and create a great potential for major disaster. Many pressures are on the operator to avoid responsibility for creating this situation.

As the investigation proceeded, increased attention was focussed on the missing information to the operator which forced solution of the problem to depend so heavily on the operator's experience and judgment. The nature of the problem can be described as follows. When in flight an aircraft is under the influence of

two sets of forces, those aerodynamic forces created by motion through the air and those inertial forces related to the motion in the gravitational field. In still air and steady flight these forces are in balance. In maneuvering flight the operator deliberately upsets this balance to produce accelerations of the mass to achieve a new state of balance and operating conditions; much of the operator's training and much of the information provided are directed at achieving these changes in state in a smooth and safe manner. In non-still air, wind shifts in velocity or direction can be sensed only weakly by the operator since instrumentation for this purpose is poor and the slow inertial response to the imbalance does not provide strong kinesthetic cues, which in any event, lag substantially the initiation of the force imbalance. In cruising flight these effects are recognized as "turbulence" and, while causing substantial diversions of the flight path, are seldom more than an annoyance. Quite the reverse is true, of course, when in close proximity to the ground where flight path diversion can cause landing off the runway. Even after the operator can sense the change in motion due to a change in wind direction or strength, a significant period of time will elapse before his corrective control inputs will overcome the inertia of the mass and take effect.[6]

Analysis of the accident made it clear that additional information must be provided the operator that would enable him to counter the effects of wind shift before the flight path was affected if disasters were to be avoided under the crowded conditions developing around major airports. An intensive series

of investigations into the problem was instigated. Ground detection of wind shift was easy but the time lag between detection, communication and corrective action by the operator proved excessive. The most promising solution appears to lie in instrumentation which can sense very small changes in the total energy of a supposedly stable system and display these in a form that proper corrective action can be taken before the changes lead to disaster. The final solution has not been reached, in part because it represents one more piece of information being supplied an operator already confronted with an information overload problem, as discussed elsewhere.

The broader lesson in this experience of management of a sophisticated system should not be overlooked. As demands on the system to operate at peak efficiency increase, minor distrubances, which could be handled easily within the flexibility of a lower demand system, can become the cause of a major disaster. To prevent this, system operation analysis must be projected forward to reveal the impact of any system disturbance under high demand situations to be certain the operator is given adequate information to respond in a timely and effective manner.

Case 6 - Inadequate Training in Hazardous Operations

On March 30, 1967, a four engined jet transport crashed during final approach to New Orleans International Airport. Six persons on board the aircraft were killed and 13 on the ground were killed.[7]

The aircraft was being used in a training exercise, an accepted operational training procedure wherein the trainee operator was

required to demonstrate his ability to maintain control of an aircraft in the face of major system malfunctions. The long established practice was for a government inspector to deliberately create a malfunction, observe the trainee's reaction to this and remove the malfunction at such time as the trainee had demonstrated his ability or inability to respond properly to the emergency. On the basis of this observation the trainee's qualification for commercial operations was established. In this regard a trainee could be either a new applicant for an operator's position or an established operator whose recent experience did not include exposure to malfunctions.

Accidents associated with training procedures were not new or rare. For the most part, however, training exercises and accidents associated with them had occurred at sites where the public was not involved and the disasters tended to be accepted as a hazard of the trade. The heavy involvement of the public in the subject accident focussed attention on the hazards of these procedures; action to minimize or eliminate these hazards was demanded. Two principal solutions were put forth, first to establish national training centers where these exercises could be conducted without hazard to the public and second, to provide national support to the development of simulation techniques which would enable hazard training to be carried out safely and adequately.

The use of simulation for training purposes had been proposed by advocates for many years. Some success had been achieved in the use of "procedural" trainers; these had served to acquaint operators with the routine of performing relatively simple tasks

associated with normal operation. Resistance and opposition to the use of simulation to train operators to handle sophisticated tasks, and particularly those associated with emergencies, was high. It was argued that under conditions of stress the operator used all his sensory mechanisms to resolve a problem and that it was impossible to provide artificially all of the cues the operator would find in the real world; in particular it was argued that it would be impossible to provide the false or misleading cues the operator must learn to ignore if the emergency was to be countered successfully.

Development of simulation techniques, however, had been spurred by other demands. New aerospace systems were being proposed for which no operating experience existed. Simulation provided the only possibility of assuring that control of these systems was possible by human operators; notable cases where simulation played this role were the supersonic transport and Apollo spacecraft design and development. Forced by these demands, intensive research efforts were devoted toward an understanding of human sensing systems and response to various sensory cues.

With this background it became possible for government regulatory groups to put forth tentative conditions for which simulation experience and demonstration could be accepted as a substitute for the same thing in the real world. Within a relatively short time it had been demonstrated that properly developed simulation was an adequate substitute, not only for training for hazardous situations but also for training for normal operations.

Today each new system development includes the development of an associated simulator. Nearly all training associated with the introduction of a new system is carried out through simulation as well as all training related to hazard avoidance and control.[8,9]

Simulation of aerospace systems probably represents the highest degree of simulation sophistication required. Techniques for duplicating all human stimuli are required. With the success achieved to date it is probable that the required information exists to produce adequate simulation for any sophisticated system; already this knowledge has been applied to train the operators of super-tankers. The experience of the aerospace systems operators has demonstrated that not only is simulation an effective means of avoiding hazards and disasters but also an economic one even where cost of simulation development is high. There is little doubt that this experience should be applied to the reduction of hazard and prevention of disaster in other highly sophisticated systems. Given the wealth of background information and experience from the aerospace industry, the simulation requirements of other systems should be easily established and met.

Case 7 - Anticipating and Mitigating Hazardous Events

In the background to this phase of the analysis it was stated that efforts were under way to develop anticipatory techniques for exposing potentially disastrous situations. These have taken several forms, simulation being prominent among them; simulations of aircraft, of the air traffic control system and combinations of the two have been developed and applied with considerable success. The success depends, however, to a considerable extent on the

ability of the simulation modeler to include all those real world factors which can combine to create the hazardous situation to be studied. In recognition of this weakness, two federal agencies, FAA and NASA, together with the industry and operators groups initiated a program to collect data on a regular basis which could be analyzed in a form to detect incipient problems.

This concept was not new. For many years the FAA had required that reports of all system failures be reported independent of any related accident. This had been extremely successful in uncovering system technical weaknesses before disasters occurred. This success created a difficult problem in initiating the new program. As technical weaknesses were isolated and eliminated, an increasing number of accidents were traced to operator errors and the question arose as to whether these were in fact human errors or whether they resulted from design features making human error inevitable. This problem was compounded by the fact that severe penalties were imposed on an operator accused of errors in operation whether or not these errors led to an accident. Thus the operator faced the risk of having penalties imposed if he reported difficulties even though, in fact, the system design or operation were imposing a near-impossible task on a well trained, but human, operator. Also, those offices charged with maintaining safety through application of penalties considered that any penalty-free reporting system would provide an all-too-easy escape from errors in judgment or skill that should be penalized. Despite these serious administrative problems, a method of operation was negotiated

which was accepted as providing an adequate safeguard to the responsibilities of the various groups involved and approximately a year after the program was proposed it was adopted on a trial basis. Since 1975 when the program went into effect it has proved exceedingly effective and is established on a permanent basis with but few modifications. Note has been taken of this success by some other industries responsible for operating sophisticated technical systems and tentative actions have been taken to initiate similar programs. The lessons learned to date in the establishment and operation of this program should be of major interest to all groups responsible for mitigation and research related to disasters.

In essence the program entails the reporting of any disturbing incident by any operator in any part of the system which is considered to presage a disaster. Anonymity is assured the reporter in all but the rarest cases. These reports are correlated and analyzed in a manner to reveal an unsuspected problem and the groups involved agree on corrective action before a disaster occurs. Just one example of the activity will be examined here to illustrate the process and its effectiveness. It should be noted that the program entails handling and processing a great deal of trivial and/or incorrect reporting and its success depends heavily on the abilities of those responsible for the analysis.

The case chosen is reported in a NASA Technical Memorandum.[10] The problem in question is that of interaction between ground

control and aircraft operator during the operation involving a specified descent profile into given airports. In past years the approach path to landing has generally been a long, shallow angle approach along the glide-slope, providing the operators ample time to stabilize the operation after changing the state of the system from its steady state cruise. This has proved to be an undemanding maneuver, leaving ample margin-of-safety for any unforeseen events. In recent years two forces have created pressures to alter this procedure. The first is noise; the shallow approach is made with considerable power, exposing large populations to excessive noise. The second is fuel cost; a steeper descent is made more quickly and with less power. Under these pressures, the FAA initiated in 1976 a program at selected airports to incorporate steep descents into the operation and gain information regarding wide application. It was recognized that different descent profiles would be required at different airports and the operator would be faced with the additional task of "capturing" the glide slope and stabilizing the aircraft for landing in a shorter period. The ground operation had the additional problem of providing proper information during the new operation.

Although no accidents have been traced to this operation, the reporting system began receiving related reports and found 59 in the first 9 months of 1977. The analysis was able to identify 4 major groupings of the sources of difficulty, from which the necessary mitigation efforts could be established. Modifications

of the operation were immediately made, removing the most likely potential cause of disaster while research proceeded to define methods of achieving the objectives without decreasing safety. This is but one of a number of problems that the program has identified as potential disaster sources. There is little doubt that this approach to mitigation is proving exceedingly effective and could be applied with equal success more widely.

Conclusions

From the examples discussed in the foregoing, several basic principles in disaster prevention can be cited:

(1) New design features, introduced to improve efficiency or flexibility of operation, must not create new problems when long established operating procedures are followed unless clear warning of these new problems is always available to the operator. (Cases 1, 2 , 3).

(2) Information to operators regarding incipient development of a problem must be treated as an integrated activity so that warning techniques are not ignored through ambiguity or confusion stemming from operator overload. (Cases 4, 2).

(3) Human sensing limits must be understood clearly and augmented where required; this must be examined with special care where new system demands remove system flexibility and once-adequate solutions to problems become unusable. (Cases 5, 3).

(4) Training for operation of complicated technical systems, particularly for disaster avoidance, cannot be achieved satisfactorily through use of the systems themselves; this is particularly true in training for hazardous operations where only through the use of advanced simulation can the exposure to multi-problem, real

world situations be given the operator without hazard. (Cases 6, 4, 3).

(5) Analysis of incident reports from routine operations will reveal potential disasters and enable mitigation before these occur; techniques for gathering and processing information without infringing on regulatory or proprietary rights are in an advanced stage of development. (Case 7).

REFERENCES

1. "Loud & Clear", Robert J. Serling, Dell Pub. Co., 1969
2. NTSB Report #AAR-75-16
3. NTSB Report #AAR-79-7
4. "Resource Management in Present and Future Aircraft Operations", Curry, R. E. and Lauber, J. K. - Presented at Conference on Aircrew Emergency Decision Training, San Francisco, CA. Nov. 1978
5. NTSB Report #AAR-76-8
6. "Investigation of CTOL Piloting Techniques for Coping with Wind Shear in Terminal Flight Operations." Interim progress report No. 1, NASA Contract NAS-10120, Systems Technology Inc., March 1979.
7. NTSB Report #AAR-File 1-0003, Dec. 20, 1967
8. Lockheed Report - 28097 for DOT/FAA, Mar., 1977
9. "Piloted Aircraft Simulation, Concepts and Overview." Sinacori, J. B., System Technology, Inc. Report Number 1074-2 (NASA Contract NAS2-9024)
10. NASA TM 78476, April, 1978

LIABILITY AND REGULATION

General Considerations

Previous sections of this report have emphasized the developing and continuing high level of scientific, technical and management attention which has been devoted to mitigating hazards in the air transport system over its history. As a result, by 1962, for the first time in air transport history, the passenger fatality rate per 100,000 passenger miles was less than 1. The rate was .94 for the world as a whole and only .38 for the United States.

Correspondingly, over the past thirty years there has been a steady decline of the idea that aviation is an ultrahazardous activity. As a result, the imposition by the courts of strict liability (absolute liability or liability without fault) for damage suffered has diminished. That trend is also evidenced by the changing pattern of statutes in the states. During the early stage of aviation development, the question of liability was greatly influenced by statutes. In 1921, a uniform state aeronautics act was drafted and approved by the Commissioners on Uniform State Laws. Section 5 of that law provided:

> "The owner of every aircraft which is operated over the lands or waters of this State is absolutely liable for injuries to persons or property on the land or water beneath, caused by the ascent, descent or flight of the aircraft, or the dropping or falling of any object therefrom, whether such owner was negligent or not, unless the injury is caused in whole or in part by the negligence of the person injured, or of the owner or bailee of the property injured. If the

> aircraft is leased, at the time of the injury to person or property, both owner and lessee shall be liable, and they may be sued jointly, or either or both of them may be sued separately. An aeronaut who is not the owner or lessee shall be liable only for the consequences of his own negligence..."

By the mid-fifties approximately 20 states had enacted some form of that statute. However, since then most states have repealed such statutes if they had them. Today most states have no applicable statute, some have statutes imposing ordinary rules of tort laws, or statutes creating a rebuttable presumption of liability against the aircraft owner and lessee.

The general trend has been to apply the concepts of negligence applicable to other types of activity to aviation activity. Aviation activity has resulted in the imposition of liability on the aircraft owner and the air carrier. In addition, more recently, such activity has resulted in imposing liability on manufacturers of aircraft and its components for damage as a result of inherently unsafe design or construction of an aircraft, or as a result of inadequate inspection.

The doctrine of res ipsa loquitur has also been introduced into the scheme of legal liability of commercial air carriers. Professor Prosser, in his universally acclaimed work, Handbook of the Law of Torts presents this doctrine as follows:

> " Negligence may be proved by circumstantial evidence. One type of circumstantial evidence, to which the courts have given the names res ipsa loquitur, arises where
>
> a. The accident is of a kind which ordinarily does not occur in the absence of someone's negligence, and

b. The apparent cause of the accident is such that the defendant would be responsible for any negligence connected with it, and

c. The possibility of contributing conduct which would make the plaintiff responsible is eliminated."*

More generally, of course, the financial tractability of sustained exposure to liability for accidents in the air transport system is dependent upon the adequate insurability at reasonable rates of the liable parties in the system, most notably the air carrier, the aircraft owners and manufacturers as noted earlier. This insurability depends in turn on the safety of the system including the reliability and availability of the safety records of the system, and the predictability of the future safety of the system. In order to deal with these considerations it is necessary first to clearly perceive the role of regulation and regulatory agencies in the air transport system.

The role of regulation and regulatory agencies has profoundly impacted on the safety of aviation in this country. Section 601 of the Federal Aviation Agency Act states the role of the Administrator of the Federal Aviation Agency with regard to safety as follows:

"(b) In prescribing standards, rules and regulations, and in issuing certificates under this title, the Administrator shall

*In the case of passengers on international air travel, the provisions of a treaty known as the Warsaw Convention, or that convention as amended at The Hague on September 28, 1955 may be applicable. For such passengers these provisions, where applicable, may limit the liability of certain carriers under contract of carriage, and this liability up to such limit shall not depend on negligence on the part of the carrier.

> give full consideration to the duty resting upon air carriers to perform their services with the highest possible degree of safety in the public interest and to any differences between air transportation and other air commerce .... The Administrator shall exercise and perform his powers and duties under this Act in such manner as will best tend to reduce or eliminate the possibility of, or recurrence of, accidents in air transportation, but shall not deem himself required to give preference to either air transportation or other air commerce in the administration and enforcement of this title."

Such authority is unusual and comparable authority to Section 601 exists in very few administrative agencies. Thus the FAA, together with the other civil aviation investigative organizations, has determined in large part the safety of civil aviation in the United States. These investigations have contributed to the understanding of, and to improvements in, flight.

Professor Billyou has stated that "the entire subject of aviation accident investigation, its methodology and use of scientific resources, compares dramatically with investigation dealing with fatal accidents in other fields of transportation."

Mr. Justice Jackson said it well in 1944 in Northwest Airlines, Inc. v. Minnesota, 322 U. S. 292, 303 (1944):

> "Congress has recognized the national responsibility for regulating air commerce. Federal control is intensive and exclusive. Planes do not wander about in the sky like vagrant clouds. They move only by federal permission, subject to federal inspection, in the hands of federally certified personnel and under an intricate system of federal commands. The moment a ship taxis onto a runway it is caught up in an elaborate and detailed system of controls. It takes off only by instruction from the control tower, it travels on prescribed beams, it may be

> diverted from its intended landing, and it obeys signals and orders. Its privileges, rights, and protection, so far as transit is concerned, it owes to the federal government alone and not to any state government."

More generally and in sum the federal government through several designated agencies has overall responsibility for the following regulations and investigative functions in the air transport system:

1. The FAA is responsible for initially certifying and periodically revalidating by tests all aircraft, flight crews and air traffic controllers plus associated equipment operating in the system;

2. The FAA is responsible for the development and continual updating of critical design criteria from a safety standpoint with support from the military service, NASA and the industry;

3. The FAA is responsible for establishing and updating equipment inspection and maintenance procedures based on operational experience reported through a formal and enforced compliance system.

4. The NTSB is responsible for oversight including accident and incident investigation to insure that early visibility and corrective actions are taken on lessons learned to avoid further hazards.

5. The CAB under the President is responsible for determining maximum allowable air fares and available routes to specific air carriers;* and finally in the area of R&D,

*Recent legislation has initiated the progressive phasing out of the CAB's regulatory functions in determining routes and fares for air carriers. This thrust, while in harmony with the principles of unrestrained competition in the free enterprise system, has raised concern in some quarters regarding the ultimate impact on flight safety and hazard mitigation.

6. The NASA will study the problems of flight to contribute to their practical solution.

It is important to note first that all of these agencies are independent from each other in the organizational structure of the federal government and they date back in their origins to as early as the First World War. Historically, therefore, they and their predecessor (e.g., NACA pre NASA and CAA pre FAA) conform in their timely assumption of responsibilities with the evolution of the air transport system. Their independence reflects careful national thought, too, to the importance of separating the the federal "carrot from the stick." Thus, for example, the independence of NACA/NASA from CAA/FAA facilitated relaxed and forthright technical relationships between industry and NACA/NASA pursuant to exploring solutions to current problems of flight and opportunities for advanced future flight capabilities, while, on the other hand, retaining openly and properly accountable relationship between industry and CAA/FAA regarding the issues of certification of new equipment in the air transport system.

More important for the purposes of this discussion, however, was the desired objective of these federal agencies to act to insure in the aggregate that the past record, the current reality, and the future predictability of safety of the air transport system would be creditable, auditable and insurable, in this order. This end result was in fact accomplished as noted by Woodhull Hay in his review of Aviation Insurance (Encyc. Am.

Vol. 2, 1955). It began in the pre-World War I time period with the initiative of Lloyds, London to issue the first policy of aviation insurance, and it gained major momentum by the end of the 20's with the beginning of commercial aviation. Thus by 1929 a number of insurance companies had entered into pooling arrangements, and underwriting groups including Associated Aviation Underwriters, United States Aviation Underwriters, and Aero Insurance Underwriters had been formed. These latter groups dominated the business to mid-century. It has long since been recognized that this business and hence the air transport business are viable in the liability insurance sense because there is close supervision and support by the federal government to insure that equipment, maintenance and personnel are of the highest quality; complete operational data are recorded and made available to the underwriters; and a much larger spread of risk is achieved than would accrue to individual owners or operators. This latter point is crucial in today's environment where large jet transports cost many tens of millions of dollars, several hundreds of passengers may travel in a single transport, and liability to the public on the ground plus third party property damage together can produce an accident exposure of unprecedented proportions in the air transport system.

This level and breadth of exposure is one which we have only recently been obliged to address in hazardous, man made, advanced technological systems. Government sponsored activities in this

arena are instructive to examine in this connection, and the remainder of this section of the report will be devoted to this subject.

Catastrophic Accidents in Government Programs

Introduction

While at present there is much legislation which has been enacted covering natural disasters no statutes have been enacted dealing with man-made governmental accidents (except for the Price-Anderson Act and a recently limited act covering NASA's space shuttle operations).

In July of 1963, a report was issued by the Legislative Drafting Research Fund of Columbia University entitled: "Catastrophic Accidents in Government Programs." The Columbia report drew on an earlier 1956-57 study by the same group for the Atomic Industrial Forum, probing the financial protection problem faced by the nuclear power program. That 1956-57 study opened the way for the 1957 Price-Anderson Amendments to the Atomic Energy Act of 1954.

The 1963 Columbia report dealt both with the legal and policy ramifications of the problem and with its technical aspects. A supporting engineering study was directed by Professor Hassialis of the School of Engineering and Applied Science of Columbia University (and Chairman of the Henry Krumb School of Mines). A portion of the engineering study, subcontracted to Arthur D. Little, Inc. of Cambridge, Massachusetts, dealt specifically with the nature and extent of the technical risks involved in a number of government programs.

The Columbia report observed that "[f]orces of unprecedented power, only recently unleashed by science, are increasingly employed or directed by the United States for governmental purposes in furtherance of the national interest" (page 7). It concluded that "[t]he possibility of devastating accidents is real and must be faced" (page 7). A two-phase program was recommended to deal with the need to protect both the public and government contractors and subcontractors by providing for interim emergency compensation as well as an ultimate remedy. Although several alternate legislative solutions were proposed, the report was clear on the point that a legislative solution was necessary in order to "provide for the consequences of a disaster before the event rather than to rely on the hope that adequate measures would be promptly enacted in the turmoil following a disaster" (page 12). The report went on to say:

> Such experience as we have affords no assurance that either industry or the public would be promptly or adequately taken care of by subsequent congressional action; in the case of the Texas City disaster, which may serve as a gauge of the speed and adequacy of what Congress might do, relief legislation did not come until eight years after the accident, and then it provided a measure of compensation which in many cases was grossly inadequate (page 12).

It appears that a legislative approach to the risk of catastrophic accidents in government programs should be considered.

Nature and Extent of the Risk

The extraordinary precautions undertaken to safeguard accidents in hazardous government programs have resulted in an

impressive safety record. No accident of catastrophic magnitude has occurred to date in the military missile programs or the space program. Yet the risk is there, however improbable. With regularity the newspapers report such unlikely happenings as missile firings and space launchings where safety devices fail to work or guidance systems malfunction.

Catastrophic accidents might arise out of government activities, such as (i) transportation of rocket fuels; (ii) firing of ground-to-air missiles concentrated in and around populated and industrial areas; (iii) weather control experiments; (iv) the unintended explosion of a nuclear weapon; and (v) chemical and bacteriological defense programs. With respect to each category the technical study of Professor Hassialis concluded that damages of a large order of magnitude are entirely credible. To again quote from the Columbia study:

> It is therefore safe to conclude that a variety of governmental activities pose the possibility of catastrophic accidents. Fortunately, the risk of such an accident with respect to any particular program and occasion appears at present to be remote. However, these programs taken together pose a significant threat of a substantial accident, and the risk multiplies as the kinds of dangerous activities and occasions for accident increase. Simple prudence would seem to dictate that consideration should be given to the impact of such accidents upon our society, and to the ways in which the losses from such accidents should be distributed (page 33).

The presence of hazards of such potential enormity becomes a matter for legislative attention because of the fact that adequate protection does not exist either for the public or for government contractors and subcontractors.

Legal Remedies

In the event of a catastrophe arising out of a government program, compensation to injured members of the public would ordinarily depend upon establishing liability for damages. A direct action against the government is circumscribed by the Federal Tort Claims Act, which requires proof of negligent or wrongful acts by employees of the government (which would not include employees of a government contractor). Even assuming that proof of fault can be established, the "discretionary function" exception makes this remedy quite uncertain.

The injured party, therefore, might be forced in many cases to attempt to establish liability on the part of one or more contractors. However, the problems of proof can be staggering. The programs would in all probability be highly technical in character and in many cases classified. The salient facts might be identifiable only by the government and industry participants in the program. The defendant manufacturers or contractors would, to conserve the resources of their shareholders, be obliged to defend claims with the utmost vigor. As the Columbia study observes:

> The complexity of the programs and of the relationships between the government and numerous prime contractors, subcontractors and suppliers would often make it difficult to trace the cause of the accident, to identify the responsible actor, and to prove his liability in a lawsuit (page 34).

A key recommendation of the Columbia study is that provision should be made in any legislation for interim relief under which prompt and effective compensation would be paid while the

specific liabilities and damages were being settled in the courts. This recommendation is particularly important because of the possibility of protracted litigation.

The situation currently facing the government contractor is also most unsatisfactory. In the case of an operating contractor, the concept of absolute liability in tort law where an "ultra-hazardous activity" is involved opens up the possibility that the operating contractor in a hazardous program may be found liable merely upon establishment of causation.

The companion development of the law governing products liability sharpens further the exposed position of a company supplying equipment or services for a government program. Starting with Mac Pherson v. Buick Motor Co., 217 N. Y. 382, 111 N.E. 1050 (1916), the manufacturer or assembler of a product has increasingly become subject to liability for harm or damage caused by his product. Moreover, liability would be joint and several, which would mean that one company might be liable for all damages to all claimants even though a number of other industrial concerns and government employees and officials had participated in the work of the program. The supplier of a component part, the furnisher of faulty design specifications, the systems contractor who fails to detect a faulty compone.. may each be found jointly and severally liable.

Nor will inspection and acceptance by the government exonerate a company from such liability. Two cases illustrate the extent to which the law has developed in extending the application

of the MacPherson case. In Boeing Airplane Company v. Brown, 291 F.2d 310 (9th Cir. 1961), the court held the manufacturer of a plane operated by the Air Force liable for the death of an Air Force Major. Although the explosion and crash were the result of a malfunction of a component furnished by another company, Boeing was held negligent in assembling the airplane with an inadequate component.

Again, in Sevits v. McKiernan-Terry Corporation, 264 F. Supp. 810 (S.D.N.Y. 1966), the court sustained a complaint against a manufacturer by a Navy crew member based on injury sustained aboard a U. S. naval aircraft carrier. The court held that a component manufacturer could be liable even without proof of negligence.

The Sevits case illustrates the development of the doctrine of strict liability in cases involving alleged defects in manufactured products. Beginning with Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (Sup. Ct. N.J. 1960) and continuing with the 1963 California Supreme Court case of Greenman v. Yuba Power Products, Inc., 377 P.2d 897, the courts have increasingly held manufacturers liable without proof of negligence. Goldberg v. Kollsman Instrument Corp., 12 N.Y. 2d 432 (1963); Prosser, The Fall of the Citadel, 50 Minn. L. Rev. 291 (1966); Restatement (Second) Torts, sec. 402A.

Financial Protection

Thus, while the government contractor or supplier occupies a very exposed position in the event of a catastrophe, at the same time, injured members of the public have an uncertain remedy. This

uncertainty is increased by the fact that available insurance protection is limited in amount and does not approach the amount of coverage required to protect a company against a very large incident where claims in the aggregate might exceed $500 million. Not many companies would be able to survive such a liability, and the injured public would, in such event, not be able to collect damages.

Insurance coverage in amounts above $10 million is acquired by relatively few companies. Whatever the maximum amount of insurance obtainable by the very largest companies today may be, it is evident that it falls far below the potential liability of companies engaged in hazardous government programs.

Current Statutory Framework

The problem discussed in the preceding pages was, of course, the reason why the Price-Anderson amendments to the Atomic Energy Act were made applicable to AEC contractors and subcontractors as well as to licensees. The Price-Anderson provision (section 170d), however, is limited to nuclear incidents arising out of or connected with AEC contractual activities or joint programs in which AEC is a participant, such as the nuclear Navy program.

"Research and Development" Indemnity Authority of DoD. The Department of Defense has had available to it since 1952 authority to indemnify its research and development contractors against claims arising out of direct performance of their contracts which result from risks defined in the contracts as "unusually hazardous" (10

U.S.C., sec. 2354). This statutory authority embraces only the military departments, and thus has no application to hazardous programs conducted by other agencies of the government such as NASA. It has also proved troublesome in other respects. It extends only to research and development contracts, and not to follow-on production contracts, which has created problems of definition and application. It depends on negotiation on both its applicability and the specific terms of indemnification coverage. This has led to inconsistent treatment as between different departments and even within the same department. Section 2354 also contains ambiguities both with regard to the limiting words that claims must "arise out of the direct performance of the contract" and with regard to the coverage of lower tier subcontractors and suppliers. Moreover, there are no provisions comparable to the 1966 amendments to the Price-Anderson Act designed to provide prompt and assured compensation to injured members of the public.

These problems led the Department of Defense to seek other legislative authority under which to indemnify its contractors engaged in hazardous programs. This occurred in two ways.

First, for several years DoD sought comprehensive indemnification legislation from the Congress. These efforts made no headway.

Secondly, the military departments turned to the use of Title II of the First War Power Act and, later, to its statutory successor (generally referrred to as Public Law 85-804 (50 U.S.C. 1431-1435).

Public Law 85-804. This statute does not explicitly deal with the indemnification of contractors, but its legislative history clearly supports its use for this purpose. Senate Report 2281 (August 9, 1958) of the Senate Committee on the Judiciary discussed the indemnity authority provided in Public Law 85-804 in these terms:

> In addition to these two specifically authorized uses of this authority, the departments authorized to use this authority have heretofore utilized it as the basis for the making of indemnity payments under certain contracts. The need for indemnity clauses in most cases arises from the advent of nuclear power and the use of highly volatile fuels in the missile program. The magnitude of the risks involved under procurement contracts in these areas have rendered commercial insurance either unavailable or limited in coverage. At the present time, military departments have specific authority to indemnify contractors who are engaged in hazardous research and development, but this authority does not extend to production contracts (10 U.S.C. 2354). Nevertheless, production contracts may involve items, the production of which may include a substantial element of risk, giving rise to the possibility of an enormous amount of claims. It is, therefore, the position of the military departments that to the extent that commercial insurance is unavailable, the risk of loss in such a case should be borne by the United States. The Atomic Energy Commission now possesses similar indemnification authority by virtue of the enactment of the Price-Anderson Act last year (Public Law 85-177).

However, Executive Order No. 10789, which implemented Public Law 85-804, conditioned the exercise of authority under it by the phrase, "within the limits of the amounts appropriated and the contract authorization provided therefor."

Thus, the usefulness of Public Law 85-804 as authority to provide indemnification was substantially undermined, in spite of the legislative history. The very need for specific statutory authority in order to extend indemnity coverage to contractors arises by virtue of the prohibition placed on government agencies by the Congress against obligating the government beyond available appropriations (cf. sec. 170j. of the Atomic Energy Act).

The Executive Order limitation in effect required agencies using this authority to make any indemnification agreement "subject to the availability of appropriations." Such a contractual undertaking is quite unclear as to its legal effect. In fact, NASA adopted a policy against the use of Public Law 85-804 for indemnification purposes because of this lack of clarity.

Other Legislative Efforts. A final point to note with regard to legislation dealing with the problem of catastrophic incidents is that in 1961 NASA submitted to the Congress a bill that would have extended to it indemnification authority comparable to that of DoD. A revised bill passed the House in that year. At hearings in the Senate, the bill was revised along the lines of the Price-Anderson Act, but no further consideration has been given to that or any similar bill by the Congress since that date.

Starting in 1964, DoD and NASA collaborated in the drafting of a comprehensive bill government-wide in scope, that followed to a large extent the thinking of the Columbia study. The bill was circulated by the Bureau of the Budget throughout the Executive Branch and thereafter was further revised to accord more closely with the

Price-Anderson Act approach. Further action was suspended on the bill.

Inadequacies of Existing Statutory Authority

The Columbia report, after a comprehensive analysis of the statutory and case law, arrived at the following conclusion:

> We have found that under present law there is no assurance of compensation to the victims of a catastrophic accident; at the same time contractors are exposed to the danger of devastating liabilities with no sure means of guarding against them (page 71).

This conclusion remains valid today in spite of certain developments since issuance of the Columbia report in 1963. The 1966 amendments to the Price-Anderson Act comprise an important development. Under them the AEC was authorized to require incorporation of provisions in insurance policies and contracts, furnished as proof of financial protection, that waive "any issue or defense as to the conduct of the claimant or fault of persons indemnified." This amendment thus allows a contractual indemnity to become a far more certain form of protection for the injured public, approaching in effectiveness the remedy of direct suit against the government upon a mere showing of causation, which had been the Columbia study's first choice for a legislative solution but which would have encountered vigorous opposition from several quarters.

The 1966 amendments also added a provision authorizing emergency assistance payments, a key recommendation of the Columbia report as we have noted above.

The inadequacies of present statutory authority can be

summarized briefly.

First, there is no clear Congressional policy encouraging widespread use of the indemnity power, comparable to that which the Joint Committee established for the Atomic Energy Commission in enacting the contract indemnity provisions of section 170d. of the Price-Anderson Act. Because they do not operate within a clear framework of Congressional policy as does AEC (now Department of Energy), agencies such as the military departments have treated indemnity as a matter of contract-by-contract bargaining. As a result, the administration of 10 U.S.C sec. 2354 and of Public Law 85-804 has been sporadic, limited, and inconsistent both as among agencies and as among contractors.

In short, the first major problem with existing statutes is that the agencies feel under no mandate to use them, and as a result they are not used widely or to full effect.

Second, because the use of the indemnity authority under existing law is a matter of contract-by-contract bargaining, it is next to impossible for subcontractors and suppliers to obtain indemnity protection. The technique of the Price-Anderson Act which automatically extends the coverage of prime contract indemnities to all subcontractors and suppliers of the project, has not been incorporated in the provisions of 10 U.S.C. sec. 2354 or Public Law 85-804.

Third, several agencies that conduct programs of a hazardous character are either ignored or inadequately covered. Examples are NASA, the Department of Commerce, and the Department

of Transportation. At the same time, existing legislation is overlapping.

Fourth, neither the military research and development statute nor Public Law 85-804 has any provision for interim relief for the injured public, unlike the Price-Anderson Act. Neither statute provides for waiver of defenses, again unlike the 1966 amendments to the Price-Anderson Act, which means that the injured public has a far less certain remedy under these statutes.

Fifth, another point is that neither statute provides for a ceiling on the Government's indemnity obligation with the related limitation of liability.

Sixth, both statutes are silent with regard to the matter of required financial protection. This places the important policy question as to required insurance entirely up to the decision of each individual government agency. Such a situation invites inconsistent treatment as between the various agencies and may well warrant more comprehensive attention and oversight.

Conclusions

In concert with continued comprehensive research, a carefully regulated and recorded program to control the overall design, development and operation of the air transport system has served to rigorously and reliably mitigate the hazards inherent to the system. AS a result, aviation has long since ceased to be viewed as ultra-hazardous and liabilities attendent to this activity are regularly and widely insured against.

This activity is, however, with the advent of jumbo jets,

markedly increasing the magnitude of the exposure of human life and property both inside and outside the aircraft to risk of serious accident. Continued trends in this direction may "together produce a catastrophic exposure of unprecedented proportion." This level of exposure is one we have only recently had to address in hazardous, man made advanced technological systems. An examination of government sponsored activities in this arena reveals that there are inadequacies of present statutory authority in the use of indemnity power, and that in the end the important policy question as to required insurance is entirely up to the decision of each individual government agency. Such a situation may well warrant more comprehensive attention and oversight.

PRINCIPLES AND POTENTIAL APPLICATIONS

From the preceeding analyses of the design through operation phases of the air transport system and the evolving considerations of liability and regulation of the system, some general principles of hazard mitigation that are potentially applicable to other advanced technological systems may be summarized as shown in the following areas.

Design, Construction, Inspection and Maintenance

- Complex engineering systems require precise design criteria carefully related to the expected operational environment.
- Design criteria should reflect, whenever possible, the total anticipated operational experience in a statistical sense, not just the expected peak values.
- Modern design tools permit designers to design complex engineering systems closer to precise design criteria thus making critical the importance of well conceived design criteria.
- A philosophy of design verification is necessary. When new technologies are employed beyond those which have been demonstrated, designers must identify and weigh the risks.
- High levels of manufacturing quality control are absolutely essential for safety and reliability.
- For hazard mitigation a uniformly high level of performance is required in design, construction, inspection and maintenance.

System Development and Operation

. To operate effectively, efficiently and safely requires people familiar with and actively involved with every critical element of the system. They must know how the existing system operates. This involves:

  - System wide engineering
  - System management by experienced system managers

. Extreme care must be taken to establish the system characteristics that in turn establish the boundaries where a system may go unstable or uncontrollable and to determine the margins of safety which must be maintained in order that transients do not result in exceeding these boundaries.

  - System simulation and training are required to establish precise operating procedures to assure recovering if unexpectedly large transients occur during the operation close to the boundary.

. Systems in operation must provide the essential information that the operators need to understand whether or not the system is operating within its design parameters for safe operation. If this is not the case it is not known what actions are required, if any, in terms of both automatic and human intervention! In addition, the information system must not provide more information than the system operators can effectively use (information overload phenomena).

  - The information system must consider the limits

of human sensory capabilities.

- Opportunities exist to combine alerting systems to cope with information saturation. This involves combining alerting devices to serve multi-purposes and in setting priorities for alerts so that only those of primary concern to the particular operating states of the moment are armed.
- Information required of the system in emergency operations must be clearly and unambiguously presented and should to the extent possible be used during all normal operations so familiarity is maintained.
- Basic human sensory capabilities which may be misleading under emergencies should not be allowed to become a normal source of information during routine operations.
- New capabilities or modifications of the system require a systematic analysis of communications and communication procedures to ensure that double meaning with the resulting ambiguity does not occur.
- Introduction of a new characteristic into an established system must be done in such a manner as to not alter the cues used by the operator to manage the system safely and in the process observe the information required to avoid disaster.
    - Even the most beneficial system changes must be examined critically in the light of prior operator experience and tendencies to revert to intuitive actions under stress.
- Human factors analysis is critical to the safe operation of

high technology systems. Several critical questions must be analyzed and answers found:

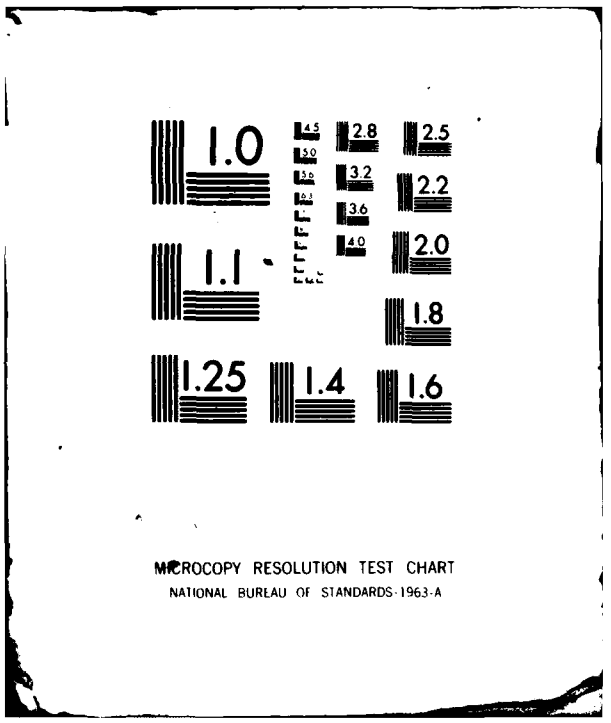
1. How is the ranking of authority established and accepted so it does not break down under stress?
2. How is the division of responsibility specified so that even under stress, routine activities continue and are not overlooked to aggravate a problem?
3. How is training conducted so that these established procedures are not disrupted by varying groups of operators which may contain personality clashes?

. As demands of a system to operate at peak efficiency increas minor disturbances, which could be handled easily within the flexibility of a lower demand system, can become the cause of a major disaster.

    - To prevent this, system operations analysis must be projected forward to reveal the impact of any system disturbance under high demand situations. This is to ensure that the operator is given adequate information to respond in a timely and effective manner.

. Simulation experience and demonstrations can be an effective substitute for the same thing in the real world. This can be done for regular training for hazardous situations as wel as normal. It is now likely that the required information exists to produce adequate simulation for most any sophistic system.

AD-A089 204 RANN INC PALO ALTO CA F/G 13/12
EXPLORATORY STUDY OF HAZARD MITIGATION AND RESEARCH IN THE AIR --ETC(U)
MAR 80 R L BISPLINGHOFF, P G DEMBLING EMW-00432
UNCLASSIFIED NL


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

- It is now feasible to design data collection systems and the related analysis that can detect incipient system failure problems before they occur.

Liability and Regulation

- The system must be continuously regulated, audited and demonstrated to be safe to the degree necessary to protect the public interest including enabling adequate insurance of the manufacturers, owners and operators of the system liable for losses of people and property potentially exposed to accidents in the system.
- Trends in the direction to "produce a catastrophic exposure of unprecedented proportion"have only recently become of concern in man made advanced technological systems. Certainly in government programs if not elsewhere such eventualities warrant more comprehensive attention and oversight in the public interest.

It is evident from examination of these principles that they are particularly suited to hazard mitigation in systems with the following characteristics:

- Subsystems and pieces designed and developed by many different specialists
- Complex interactions and interdependence of subsystems
- Human factor - machine interfaces at several points
- Critical tradeoffs between system efficiency, safe operation, and economic factors.

Examples of technology based systems which have several of these characteristics and to which the general principles may apply include:

- Complex gas, oil, slurry pipeline systems
- Super tanker and LNG transportation systems including loading, unloading and related matters.
- Movements of substantial amounts of hazardous materials through a multi-modal transportation system.
- Generation and transmission of electrical power through an extensive grid involving multiple power sources including fossil, nuclear, hydro, solar and others.

It is clear from the three major reports[1-3] on the Three Mile Island nuclear accident that a number of the hazard mitigation principles developed in the air transport system may not have been fully followed. These may include the areas of regular training, effective communications, and rigorous incident as well as accident investigation and reporting of emergency situations. It is also clear that had these principles been followed, Three Mile Island might not have occurred, or if it had, it would have been less severe. These are probabilities not assurances. What is generally required is the conduct of comparative analyses of specific technology based systems against the hazard mitigation principles and concepts derived from experience with the air transport system to determine their specific applicability.

REFERENCES

1. Rogouin, Mitchell, Three Mile Island, Nuclear Regulatory Commission Special Inquiry Group, Vol. 1, January 1980

2. National Academy of Public Administration, Major Alternatives for Government Policies, Organizational Structures, and Actions in Civilian Nuclear Reactor Emergency Management in the United States, January 1980.

3. Report of the President's Commission on The Accident at Three Mile Island, October, 1979.